PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-211358
(43)Date of publication of application : 31.07.2002

(51)Int.Cl. B60R 25/04
B60R 25/10
G01C 21/00
// H04L 9/32

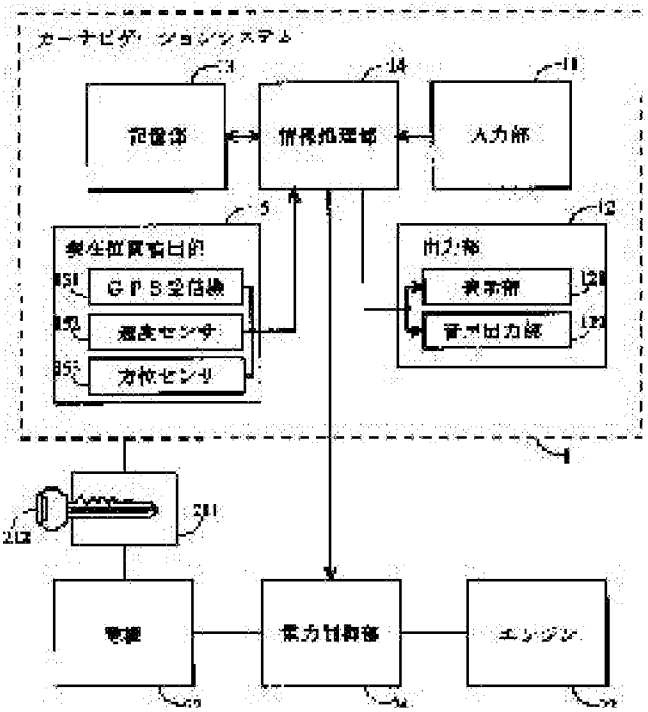
(21)Application number : 2001-270924
(22)Date of filing : 06.09.2001

(71) Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : ATA TERUAKI
SAKAMOTO KIYOMI
YAMASHITA ATSUSHI
HAMADA HIROYUKI

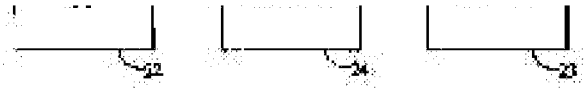
(30)Priority
Priority number : 2000349875 Priority date : 16.11.2000 Priority country : JP

(54) AUTHENTICATION DEVICE AND AUTHENTICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an authentication device for authenticating a just user maneuvering a vehicle allowing its miniaturization and reduction of cost and having high safety by an unprecedented authentication method.
SOLUTION: A current position detection part 15 detects vehicle history information changing in accordance with the use of the vehicle, and a storage part 13 stores the vehicle history information. When authentication is performed, an output part 12 gives a question about the vehicle history information, and the user inputs an answer for the question through an input part 11. An information processing part 14 determines whether the question is right or not



based on the vehicle history information stored in the storage part 13 and the user's answer to authenticate the just user of the vehicle.



* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]A vehicle-history-information primary detecting element which is an authentication device for attesting a valid user of vehicles, and detects vehicle history information which changes with use of said vehicles, A vehicle-history-information storage which stores vehicle history information detected by said vehicle-history-information primary detecting element, An outputting part which outputs a question about said vehicle history information, and an answer input part which inputs a reply of a user to a question about said vehicle history information, An authentication device provided with an user authentication part which attests that it is a valid user based on vehicle history information stored in said vehicle-history-information storage, and said user's reply.
[Claim 2]The authentication device according to claim 1 with which said vehicle history information includes point hysteresis information showing a history about one or more specified points.
[Claim 3]The authentication device comprising according to claim 2:
Time which passed through said register point last time about one or more register points where said point hysteresis information was beforehand registered by said user.
Information about time which took said vehicles last time.

[Claim 4]From said register point, said user authentication part elects arbitrary points, and said outputting part, The authentication device according to claim 3 outputting a question of time passed when said vehicles were taken last time when said vehicles are taken last time with a question whether to have passed about a point elected by said user authentication part when said vehicles were taken last time and it passes.
[Claim 5]The authentication device according to claim 3 which said answer input part inputs a point where said user was selected among said register points, and is characterized by said outputting part outputting a question of time passed about a point inputted in said answer input part when said vehicles were taken last time.
[Claim 6]Have further a personal information storage which stores personal information containing a password beforehand set up by peculiar information about said user, and/or said user, and said outputting part, When a lapse period after taking said vehicles last time is less than a prescribed period, When a question about said vehicle history information is outputted and said lapse period exceeds said prescribed period, Output a question about said personal information and said answer input part, When said lapse period is said less than prescribed period, When a reply of a user to a question about said vehicle history

information is inputted and said lapse period exceeds said prescribed period, Input a reply of a user to a question about said personal information, and said user authentication part, When said lapse period is said less than prescribed period, The authentication device according to claim 1 attesting that it is a valid user based on said personal information and said user's reply when it judges whether it is a valid user and said lapse period exceeds said prescribed period based on said vehicle history information and said user's reply.
[Claim 7]The authentication device according to claim 1 characterized by making said power controller start electric supply when it has further a power controller which performs electric supply to an engine of vehicles and it is attested that said user authentication part is a valid user.
[Claim 8]A power controller which performs electric supply to an engine of vehicles, and a key authentication section which makes said power controller start electric supply when attestation using a key is performed and it is attested that it is a regular key, Have further a restriction command input part which inputs a use restriction command of said vehicles, and said user authentication part, The authentication device according to claim 1 forbidding said power controller from starting electric supply by said key authentication section when it attests according to a use restriction command of said vehicles and attests with it being a valid user.
[Claim 9]The authentication device according to claim 8 which is further provided with a use command input part which inputs a use command of said vehicles, said user authentication part attests according to a use command of said vehicles, and is characterized by making said power controller start electric supply when it attests with it being a valid user.
[Claim 10]A power controller which performs electric supply to an engine of vehicles, and a key authentication section which makes electric supply start to said power controller when attestation using a key is performed and it is attested that it is a regular key, The authentication device according to claim 1 further provided with a reporting part which notifies to a user that vehicles are used unjustly when it is not attested in predetermined time that said user authentication part is a valid user, after electric supply by said power controller is started.
[Claim 11]The authentication device according to claim 1 constituting as some car-navigation systems.
[Claim 12]A vehicle-history-information primary detecting element which is an input terminal and an authentication device which can be communicated which input a reply of a user to an output of a question about vehicle history information whether it changes with use of vehicles, and the question concerned, and detects said vehicle history information, A vehicle-history-information storage which stores vehicle history information detected by said vehicle-history-information primary detecting element, The communications department which transmits a question about said vehicle history information to said input terminal, and receives a reply of a user to the question concerned from the input terminal concerned, An authentication device provided with an user authentication part which attests that it is a valid user based on vehicle history information stored in said vehicle-history-information storage, and said user's reply.
[Claim 13]Are an authentication device which is carried in vehicles and attests a valid user of the vehicles concerned, the authentication device concerned, and an input terminal which can be communicated an included authentication system, and said authentication

device, A vehicle-history-information primary detecting element which detects vehicle history information which changes with use of said vehicles, A vehicle-history-information storage which stores vehicle history information detected by said vehicle-history-information primary detecting element, The communications department which transmits a question about said vehicle history information to said input terminal, and receives a reply of a user to the question concerned from the input terminal concerned, Based on vehicle history information stored in said vehicle-history-information storage, and said user's reply, have an user authentication part which attests that it is a valid user, and said input terminal, An authentication system provided with the terminal side outputting part which outputs a question about said vehicle history information transmitted from said authentication device, the terminal side answer input part which inputs a reply of a user to a question about said vehicle history information, and the terminal side communications department which transmits said user's reply to said authentication device.

[Claim 14]Said authentication device performs attestation using a key with a power controller which performs electric supply to an engine of vehicles, When it is attested that it is a regular key, have further a key authentication section which makes electric supply start to said power controller, and said input terminal, Have further the terminal side restriction command input part which inputs a use restriction command of said vehicles, and said user authentication part, The authentication system according to claim 13 forbidding said power controller from starting electric supply by said key authentication section when it attests according to a use restriction command of said vehicles and attests with it being a valid user.

[Claim 15]Said input terminal is further provided with the terminal side use command input part which inputs a use command of said vehicles, and said user authentication part, The authentication system according to claim 14 characterized by making said power controller start electric supply when it attests according to a use command of said vehicles and attests with it being a valid user.

[Claim 16]Are a vehicle side device carried in vehicles, the vehicle side device concerned, and an authentication terminal which can be communicated an included authentication system, and said vehicle side device, A vehicle-history-information primary detecting element which detects vehicle history information which changes with use of said vehicles, Have the communications department which transmits vehicle history information detected by said vehicle-history-information primary detecting element to said authentication terminal, and said authentication terminal, Terminal side-car both hysteresis information storage that stores vehicle history information transmitted from said communications department, The terminal side outputting part which outputs a question about said vehicle history information, and the terminal side answer input part which inputs a reply of a user to a question about said vehicle history information, An authentication system provided with the terminal side user authentication part which attests that it is a valid user based on vehicle history information stored in said terminal side-car both hysteresis information storage, and said user's reply.

[Claim 17]Said authentication terminal is further provided with the terminal side communications department which transmits an authentication result by said terminal side user authentication part to said vehicle side device, and said vehicle side device, The authentication system according to claim 16 further provided with an anti-theft treating part which performs processing for preventing a theft of said vehicles based on a received

authentication result from said terminal side communications department.
[Claim 18]Said anti-theft treating part electric supply to an engine of vehicles including a power controller to perform said vehicle side device, When attestation using a key is performed and it is attested that it is a regular key, have further a key authentication section which makes electric supply start to said power controller, and said authentication terminal, Have further the terminal side restriction command input part which inputs a use restriction command of said vehicles, and said terminal side user authentication part, When it attests according to a use restriction command of said vehicles and attests with it being a valid user, make said terminal side communications department transmit to said power controller, and an electric supply inhibiting signal by it. The authentication system according to claim 17 forbidding said power controller from starting electric supply by said key authentication section.
[Claim 19]Said authentication terminal is further provided with the terminal side use command input part which inputs a use command of said vehicles, and said terminal side user authentication part, The authentication system according to claim 18 making said terminal side communications department transmit a feeding signal to said power controller, and making said power controller start electric supply by it when it attests according to a use command of said vehicles and attests with it being a valid user.
[Claim 20]Said vehicle side device is further provided with a vehicle-history-information storage which stores vehicle history information detected by said vehicle-history-information primary detecting element, and said communications department, The authentication system according to claim 16 transmitting vehicle history information stored in said vehicle-history-information storage to said authentication terminal when use of vehicles is completed.
[Claim 21]An authentication device and an input terminal which can be communicated characterized by comprising the following which are carried in vehicles and attest a valid user of the vehicles concerned.
The terminal side outputting part which outputs a question about vehicle history information which is transmitted from said authentication device, and which changes with use of said vehicles.
The terminal side answer input part which inputs a reply of a user to a question about said vehicle history information.
The terminal side communications department which transmits said user's reply to said authentication device.

[Claim 22]The terminal side communications department which is a vehicle side device and an authentication terminal which can be communicated which detect vehicle history information which changes with use of vehicles, and receives vehicle history information detected by said vehicle side device from the vehicle side device concerned, Terminal side-car both hysteresis information storage that stores vehicle history information received by said communications department, The terminal side outputting part which outputs a question about said vehicle history information, and the terminal side answer input part into which a reply of a user to a question about said vehicle history information is inputted, An authentication terminal provided with the terminal side user authentication part which attests that it is a valid user based on vehicle history information stored in said vehicle-history-information storage, and said user's reply.

[Claim 23]An authentication method comprising:
A step which is an authentication method for attesting a valid user of vehicles, and detects vehicle history information which changes with use of said vehicles.
A step which stores said vehicle history information.
A step which performs a question about said vehicle history information.
A step which attests that it is a valid user based on a step which inputs a reply of a user to said question, and said vehicle history information and said user's reply.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]More specifically, this invention relates to the authentication device which attests the valid user of vehicles about an authentication device.
[0002]
[Description of the Prior Art]There is the method of putting an engine into operation as an authentication method of the valid user of vehicles from the former using a mechanical cylinder key. If this has no regular key, it prevents the theft of vehicles by making engine start impossible. However, as for the mechanical key, comparatively easily, since it can reproduce, sufficient theft preventive effect is not necessarily acquired.
[0003]As it is in JP,4-15141,B, by including specific electronic intelligence in a key, reproduction of a key is made difficult and there are some which strengthen the theft preventive effect of vehicles. However, when the theft of the regular key is carried out, the theft of vehicles cannot be prevented and a theft preventive effect cannot say also in this case that it is enough.
[0004]Then, how to prevent the theft of vehicles can be considered by judging whether you are a regular user by personal authentication. As this method, as it is in JP,7-168930, A, JP,2000-168502,A, and JP,2000-85536,A, for example, Individual collation is performed by detecting the living body feature of the iris of a fingerprint or eyes, and the user recognition device for vehicles which attests that he is a regular user is proposed. The authentication device which uses a password as a key of attestation is known from the former as other methods of attesting that he is a regular user by personal authentication.
[0005]
[Problem(s) to be Solved by the Invention]In the method of attesting that he is a regular user by detecting the living body feature, since the unit which detects the living body feature is needed, an authentication device will enlarge and high-cost-ize. On the other hand, in the method using a password, if it continues using the same password, a possibility that a password will be used by stealth will become high, and the safety of attestation will become low. Therefore, since it is necessary to change a password periodically, a user's burden becomes large.
[0006]So, the purpose of this invention is to provide the authentication device and authentication method of safety which attest the high valid user which operated vehicles by the method of the attestation which is not until now, so that a miniaturization and low-cost-izing are possible.

[0007]
[The means for solving a technical problem and an effect of the invention] This invention has the feature which is described below, in order to attain the above purposes.
[0008]The vehicle-history-information primary detecting element which the 1st invention is an authentication device for attesting the valid user of vehicles, and detects the vehicle history information which changes with use of vehicles, The vehicle-history-information storage which stores the vehicle history information detected by the vehicle-history-information primary detecting element, Based on the outputting part which outputs the question about vehicle history information, the answer input part which inputs a reply of the user to the question about vehicle history information, and the vehicle history information and a user's reply which are stored in the vehicle-history-information storage, it has the user authentication part which attests that it is a valid user.
[0009]According to the 1st above-mentioned invention, vehicle history information can be used for user authentication. By movement of vehicles, progress of time, etc., vehicle history information changes with use of vehicles, and means the information which can identify vehicles. For example, the information about a point like the history of the point through which it passed, an origin, or the destination, The information about a course like the history of the course which moved, remainder of the gasoline, the information about the speed of vehicles, and the information about a VICS (Vehicle Information and Communication System) message receiving history are included in vehicle history information. Such vehicle history information is information which only the valid user which operated vehicles has memorized, and is information which changes continuously whenever it moreover takes vehicles. Therefore, since a possibility of embezzling for others decreases compared with the case where a fixed password is used as certification information by using vehicle history information for attestation, the safety of attestation becomes high. Since it can attest without needing the detecting unit which detects the living body feature compared with the authentication device which attests using the living body feature, a miniaturization and low-cost-izing are possible.
[0010]The 2nd invention is an invention subordinate to the 1st invention, and vehicle history information includes point hysteresis information showing hysteresis information about one or more specified points.
[0011]According to the 2nd above-mentioned invention, point hysteresis information can be used for user authentication. Point hysteresis information is information as which vehicles express a history which passed before or dropped in about the point. Such point hysteresis information especially is information which can be memorized comparatively easily, even if a user is not conscious. Therefore, according to the 2nd above-mentioned invention, a burden for a user's memory can be lessened by using point hysteresis information for attestation.
[0012]The 3rd invention is an invention subordinate to the 2nd invention, and point hysteresis information includes information about time which passed through one or more points beforehand registered by user last time, and time which took vehicles last time.
[0013]According to the 3rd above-mentioned invention, a point through which a user often passes, or an institution used well can be chosen, and a history about a selected point can be used for attestation. Therefore, since the user can memorize easily a reply to a question at the time of attesting, a burden for a user's memory is eased. According to the 3rd above-mentioned invention, a question is performed about information of a day and

time which were passed last time which a user can memorize easily. A burden for a user's memory is eased by this.

[0014]The 4th invention is an invention subordinate to the 3rd invention, and an user authentication part, Arbitrary points are elected from a register point, and an outputting part outputs a question of time passed when vehicles were taken last time, when vehicles are taken last time with a question whether to have passed about a point elected by user authentication part when vehicles were taken last time and it passes.

[0015]According to the 4th above-mentioned invention, a question about a history of a point can be performed about a point which an user authentication part elected automatically. Therefore, since it is not necessary to perform operation which chooses a point, a burden of a user's operation is eased.

[0016]The 5th invention is an invention subordinate to the 3rd invention, an answer input part inputs a point where a user was selected among register points, and an outputting part outputs a question of time passed about a point inputted by answer input part when vehicles were taken last time.

[0017]According to the 5th above-mentioned invention, time passed last time can be asked about a point which a user chose himself. Therefore, since the user should just answer passage time about a point where he has memorized a history, a burden for a user's memory is eased further.

[0018]The 6th invention is an invention subordinate to the 1st invention, and is further provided with a personal information storage which stores personal information containing a password beforehand set up by peculiar information and/or a user about a user, When a lapse period after taking vehicles last time is less than a prescribed period, an outputting part, When a question about vehicle history information is outputted and a lapse period exceeds a prescribed period, Output a question about personal information and an answer input part, When a reply of a user to a question about vehicle history information is inputted when a lapse period is less than a prescribed period, and a lapse period exceeds a prescribed period, Input a reply of a user to a question about personal information, and an user authentication part, When it judges whether it is a valid user based on vehicle history information and a user's reply when a lapse period is less than a prescribed period, and a lapse period exceeds a prescribed period, based on personal information and a user's reply, it attests that it is a valid user.

[0019]According to the 6th above-mentioned invention, when a user does not take prescribed period vehicles, attestation using personal information is performed. A user will forget vehicle history information, if a period generally passes to some extent after getting on last time. In such a case, a burden for a user's memory of a direction which uses for attestation personal information which a user can memorize certainly becomes small. As mentioned above, an authentication device which ensures attestation can be provided, easing a burden for a user's memory, also when vehicles are not taken by the 6th above-mentioned invention for a long period of time.

[0020]The 7th invention is an invention subordinate to the 1st invention, and it has further a power controller which performs electric supply to an engine of vehicles, and an user authentication part makes a power controller start electric supply, when it is attested that it is a valid user.

[0021]According to the 7th above-mentioned invention, use of vehicles is attained only when it is attested that it is a valid user. Therefore, a theft of vehicles can be prevented

with an authentication device using vehicle history information.
[0022]A power controller which the 8th invention is an invention subordinate to the 1st invention, and performs electric supply to an engine of vehicles, A key authentication section which makes a power controller start electric supply when attestation using a key is performed and it is attested that it is a regular key, When it has further a restriction command input part which inputs a use restriction command of vehicles, an user authentication part attests according to a restriction command of vehicles use and it attests with it being a valid user, a power controller is forbidden from starting electric supply by a key authentication section.
[0023]According to the 8th above-mentioned invention, the authentication device can forbid use of vehicles by attestation using a key by attestation which used vehicle history information. Therefore, even if it is a case where the theft of the key is carried out, the user can prevent a theft of vehicles by performing attestation which used vehicle history information. At the time of the usual vehicles use, since the user should perform only attestation which used a key, time and effort of attestation at the time of vehicles use decreases.
[0024]The 9th invention is an invention subordinate to the 8th invention, and it has further a use command input part which inputs a use command of vehicles, and an user authentication part makes a power controller to attest according to a use command of vehicles, and start electric supply, when it attests with it being a valid user.
[0025]According to the 9th above-mentioned invention, the authentication device can enable use of vehicles by attestation which used vehicle history information. Therefore, even if a user is a case where use of vehicles by attestation which used a key is restricted, he can use vehicles.
[0026]A power controller which the 10th invention is an invention subordinate to the 1st invention, and performs electric supply to an engine of vehicles, A key authentication section which makes electric supply start to a power controller when attestation using a key is performed and it is attested that it is a regular key, After electric supply by a power controller is started, when it is not attested in predetermined time that an authentication section is a valid user, it has further a reporting part which notifies to a user that vehicles are used unjustly.
[0027]According to the 10th above-mentioned invention, only attestation using a key is performed at the time of entrainment of vehicles, and attestation using vehicle history information is performed after the beginning of using of vehicles. Therefore, at the time of entrainment of vehicles, a user is easy and should perform only attestation which can be performed in a short time. When attestation using vehicle history information is not performed, a report to a valid user is performed. Therefore, it is satisfactory even if it will not perform attestation using vehicle history information, if it is a case where a valid user uses vehicles. As mentioned above, according to the 10th above-mentioned invention, the valid user can use vehicles by easy attestation which used a key. According to the 10th above-mentioned invention, to a user who uses it unjustly, high attestation of safety using vehicle history information can be performed.
[0028]The 11th invention is an invention subordinate to the 1st invention, and was constituted as some car-navigation systems.
[0029]According to the 11th above-mentioned invention, an authentication device is constituted using a car-navigation system. A car-navigation system has a function to input

information from a user, a function which outputs information with a picture, a sound, etc. to a user, a function to memorize vehicle history information, and the function to detect a current position of vehicles. Therefore, in order to realize an authentication device of this invention, it is possible to use a car-navigation system. As mentioned above, it is not necessary to install a new device and, according to the 11th above-mentioned invention, an authentication device of this invention can be realized.

[0030]A vehicle-history-information primary detecting element which the 12th invention is an input terminal and an authentication device which can be communicated which input a reply of a user to an output of a question about vehicle history information and a question whether it changes with use of vehicles, and detects vehicle history information, A vehicle-history-information storage which stores vehicle history information detected by vehicle-history-information primary detecting element, A question about vehicle history information was transmitted to an input terminal, and it has an user authentication part which attests that it is a valid user based on the communications department which receives a reply of a user to a question from an input terminal, and vehicle history information and a user's reply which are stored in a vehicle-history-information storage.

[0031]According to the 12th above-mentioned invention, since a possibility of embezzling for others decreases compared with a case where a fixed password is used as certification information, the safety of attestation becomes high. Since it can attest without needing a detecting unit which detects the living body feature compared with an authentication device which attests using the living body feature, a miniaturization and low-cost-izing are possible.

[0032]According to the 12th above-mentioned invention, the user can perform attestation from from outside vehicles using an input terminal. Therefore, the user can perform beforehand attestation which used vehicle history information before entrainment of vehicles. Thereby, when vehicles are taken, it becomes unnecessary to perform troublesome attestation and time and effort of a user at the time of entrainment can be saved.

[0033]Are an authentication device which the 13th invention is carried in vehicles and attests a valid user of vehicles, an authentication device, and an input terminal which can be communicated an included authentication system, and an authentication device, A vehicle-history-information primary detecting element which detects vehicle history information which changes with use of vehicles, A vehicle-history-information storage which stores vehicle history information detected by vehicle-history-information primary detecting element, The communications department which transmits a question about vehicle history information to an input terminal, and receives a reply of a user to a question from an input terminal, Based on vehicle history information and a user's reply which are stored in a vehicle-history-information storage, have an user authentication part which attests that it is a valid user, and an input terminal, It has the terminal side outputting part which outputs a question about vehicle history information transmitted from an authentication device, the terminal side answer input part which inputs a reply of a user to a question about vehicle history information, and the terminal side communications department which transmits a user's reply to an authentication device.

[0034]According to the 13th above-mentioned invention, since a possibility of embezzling for others decreases compared with a case where a fixed password is used as certification information, the safety of attestation becomes high. Since it can attest without needing a

detecting unit which detects the living body feature compared with an authentication device which attests using the living body feature, a miniaturization and low-cost-izing are possible.

[0035]According to the 13th above-mentioned invention, the user can perform attestation from from outside vehicles using an input terminal. Therefore, the user can perform beforehand attestation which used vehicle history information before entrainment of vehicles. Thereby, when vehicles get on, it becomes unnecessary to perform troublesome attestation and time and effort of a user at the time of entrainment can be saved.

[0036]The 14th invention is an invention subordinate to the 13th invention, and an authentication device, Attestation using a key is performed with a power controller which performs electric supply to an engine of vehicles, When it is attested that it is a regular key, have further a key authentication section which makes electric supply start to a power controller, and an input terminal, When it has further the terminal side restriction command input part which inputs a use restriction command of vehicles, an user authentication part attests according to a use restriction command of vehicles and it attests with it being a valid user, a power controller is forbidden from starting electric supply by a key authentication section.

[0037]According to the 14th above-mentioned invention, the authentication system can forbid use of vehicles by attestation using a key by attestation which used vehicle history information. Therefore, even if it is a case where the theft of the key is carried out, the user can prevent a theft of vehicles by performing attestation which used vehicle history information. At the time of the usual vehicles use, since the user should perform only attestation which used a key, time and effort of attestation at the time of vehicles use decreases.

[0038]According to the 14th above-mentioned invention, use of vehicles can be forbidden by using an input terminal. That is, even if a user does not enter into vehicles, he can forbid use of vehicles from from outside vehicles. Therefore, use of vehicles can be forbidden even when it cannot go into in the car, since a user does not have a spare key when the theft of the key is carried out.

[0039]The 15th invention is an invention subordinate to the 14th invention, an input terminal is further provided with the terminal side use command input part which inputs a use command of vehicles, and when it attests with it being a valid user, it makes a power controller for an user authentication part to attest according to a use command of vehicles, and start electric supply.

[0040]According to the 15th above-mentioned invention, the authentication system can enable use of vehicles by attestation which used vehicle history information. Therefore, even if a user is a case where use of vehicles by attestation which used a key is restricted, he can use vehicles.

[0041]The 16th invention is a vehicle side device carried in vehicles, a vehicle side device, and an authentication terminal which can be communicated an included authentication system, and a vehicle side device, A vehicle-history-information primary detecting element which detects vehicle history information which changes with use of vehicles, Have the communications department which transmits vehicle history information detected by vehicle-history-information primary detecting element to an authentication terminal, and an authentication terminal, Terminal side-car both hysteresis information storage that stores vehicle history information transmitted from the communications department, The

terminal side outputting part which outputs a question about vehicle history information, and the terminal side answer input part which inputs a reply of a user to a question about vehicle history information, Based on vehicle history information and a user's reply which are stored in terminal side-car both hysteresis information storage, it has the terminal side user authentication part which attests that it is a valid user.

[0042]According to the 16th above-mentioned invention, vehicle history information which changes with use of vehicles is used for attestation. Therefore, since a possibility of embezzling for others decreases compared with a case where a fixed password is used as certification information, the safety of attestation becomes high. Since it can attest without needing a detecting unit which detects the living body feature compared with an authentication device which attests using the living body feature, a miniaturization and low-cost-izing of a device are possible.

[0043]According to the 16th above-mentioned invention, the user can attest outside vehicles using an authentication terminal. Therefore, the user can perform beforehand attestation which used vehicle history information before entrainment of vehicles. Thereby, when vehicles get on, it becomes unnecessary to perform troublesome attestation and time and effort of a user at the time of entrainment can be saved.

[0044]The 17th invention is an invention subordinate to the 16th invention, and an authentication terminal, It had further the terminal side communications department which transmits an authentication result by the terminal side user authentication part to a vehicle side device, and a vehicle side device is further provided with an anti-theft treating part which performs processing for preventing a theft of vehicles based on an authentication result received from the terminal side communications department.

[0045]According to the 17th above-mentioned invention, the vehicle side device can use for theft prevention of vehicles a result of attestation which used vehicle history information. Therefore, the vehicle side device can heighten a theft preventive effect of vehicles by using high attestation of safety.

[0046]The 18th invention is an invention subordinate to the 17th invention, and an anti-theft treating part, Electric supply to an engine of vehicles including a power controller to perform a vehicle side device, When attestation using a key is performed and it is attested that it is a regular key, have further a key authentication section which makes electric supply start to a power controller, and an authentication terminal, Have further the terminal side restriction command input part which inputs a use restriction command of vehicles, and the terminal side user authentication part, When it attests according to a use restriction command of vehicles and attests with it being a valid user, the terminal side communications department is made to transmit an electric supply inhibiting signal to a power controller, and a power controller is forbidden from starting electric supply by a key authentication section by it.

[0047]According to the 18th above-mentioned invention, the authentication system can forbid use of vehicles by attestation using a key by attestation which used vehicle history information. Therefore, even if it is a case where the theft of the key is carried out, the user can prevent a theft of vehicles by performing attestation which used vehicle history information. At the time of the usual vehicles use, since the user should perform only attestation which used a key, time and effort of attestation at the time of vehicles use decreases.

[0048]According to the 18th above-mentioned invention, use of vehicles can be forbidden

by using an input terminal. That is, even if a user does not enter into vehicles, he can forbid use of vehicles from from outside vehicles. Therefore, use of vehicles can be forbidden even when it cannot go into in the car, since a user does not have a spare key when the theft of the key is carried out.

[0049]The 19th invention is an invention subordinate to the 18th invention, and an authentication terminal, It has further the terminal side use command input part which inputs a use command of vehicles, and when it attests according to a use command of vehicles and attests with it being a valid user, the terminal side user authentication part makes the terminal side communications department transmit a feeding signal to a power controller, and makes a power controller start electric supply by it.

[0050]According to the 19th above-mentioned invention, the authentication system can enable use of vehicles by attestation which used vehicle history information. Therefore, even if a user is a case where use of vehicles by attestation which used a key is restricted, he can use vehicles.

[0051]The 20th invention is an invention subordinate to the 16th invention, and a vehicle side device, It has further a vehicle-history-information storage which stores vehicle history information detected by vehicle-history-information primary detecting element, and the communications department transmits vehicle history information stored in a vehicle-history-information storage to an authentication terminal, when use of vehicles is completed.

[0052]According to the 20th above-mentioned invention, hysteresis information of vehicles to last time will be stored in an authentication terminal. Therefore, since the newest vehicle history information is always stored in an authentication terminal, the authentication system can perform exact attestation.

[0053]The 21st invention is provided with the following.

The terminal side outputting part which outputs a question about vehicle history information which is carried in vehicles, is an authentication device and an input terminal which can be communicated which attest a valid user of vehicles, and is transmitted from an authentication device, and which changes with use of vehicles.

The terminal side answer input part which inputs a reply of a user to a question about vehicle history information.

The terminal side communications department which transmits a user's reply to an authentication device.

[0054]According to the 21st above-mentioned invention, an input terminal can be attested by vehicle history information by using an authentication device. That is, even if a user is a case where it is out of vehicles, he can attest beforehand. Thereby, when vehicles get on, it becomes unnecessary to perform troublesome attestation and time and effort of a user at the time of entrainment can be saved.

[0055]The terminal side communications department which the 22nd invention is a vehicle side device and an authentication terminal which can be communicated which detect vehicle history information which changes with use of vehicles, and receives vehicle history information detected by a vehicle side device from a vehicle side device, Terminal side-car both hysteresis information storage that stores vehicle history information received by the communications department, The terminal side outputting part which outputs a question about vehicle history information, and the terminal side answer input

part into which a reply of a user to a question about vehicle history information is inputted, Based on vehicle history information and a user's reply which are stored in a vehicle-history-information storage, it has the terminal side user authentication part which attests that it is a valid user.

[0056]According to the 22nd above-mentioned invention, a communication terminal performs attestation which used vehicle history information. Therefore, a possibility of embezzling for others decreases compared with a case where a fixed password is used as certification information, and the safety of attestation becomes high. Since it can attest without needing a detecting unit which detects the living body feature compared with an authentication device which attests using the living body feature, a miniaturization and low-cost-izing are possible.

[0057]According to the 22nd above-mentioned invention, the user can attest outside vehicles using an authentication terminal. Therefore, the user can perform beforehand attestation which used vehicle history information before entrainment of vehicles. Thereby, when vehicles get on, it becomes unnecessary to perform troublesome attestation and time and effort of a user at the time of entrainment can be saved.

[0058]The 23rd invention is provided with the following.

A step which is an authentication method for attesting a valid user of vehicles, and detects vehicle history information which changes with use of vehicles.

A step which stores vehicle history information.

A step which performs a question about vehicle history information.

A step which judges whether it is a valid user based on a step which inputs a reply of a user to a question, and vehicle history information and a user's reply.

[0059]According to the 23rd above-mentioned invention, vehicle history information which changes with use of vehicles is used for attestation. Therefore, since a possibility of embezzling for others decreases compared with a case where a fixed password is used as certification information, the safety of attestation becomes high. Since it can attest without needing a detecting unit which detects the living body feature compared with an authentication device which attests using the living body feature, a miniaturization and low-cost-izing are possible.

[0060]

[Embodiment of the Invention]First, the outline of the authentication device concerning this embodiment is explained. The vehicle history information used for attestation in this invention changes with use of vehicles. Therefore, there are few possibilities of embezzling, and if it attests using vehicle history information, since it is not necessary to change periodically, high attestation of safety can be performed. The information memorizable even if a user is not conscious of such vehicle history information especially is desirable. It is because the user does not need to memorize by force and the burden for a user's memory will decrease, if such information is used. Then, the authentication device concerning this embodiment attests using the hysteresis information about a predetermined point. Predetermined points are arbitrary points which a user can register beforehand here, and it is desirable to register two or more points through which a user often passes usually. Specifically, the authentication device concerning this embodiment attests by making a user answer the question whether it passed through the predetermined point when it got on last time, and about what time [of what day] it passed when it

passed. In explanation of this embodiment, the predetermined point which the user registered is called a register point.

[0061]The authentication device concerning this embodiment attests by using together the hysteresis information and personal information about a specified point. Here, personal information means information peculiar to a user. Typically, a user's date of birth, family structure, or the password that the user set up beforehand is used as personal information. The authentication device concerning this embodiment attests by using together the password which the user set to the hysteresis information about a specified point beforehand.

[0062]Hereafter, a 1st embodiment is described in detail using drawing 1 - drawing 9. Drawing 1 is a block diagram showing the composition of the vehicles carrying the authentication device concerning a 1st embodiment. An authentication device is a gestalt using the car-navigation system currently generally used in vehicles. The car-navigation system 1 is provided with the following in drawing 1.

Input part 11.
Outputting part 12.
Storage parts store 13.
The information processing section 14 and the current position primary detecting element 15.
Vehicles are provided with the following.
The key cylinder 211 and the cylinder key 212.
Power supply 22.
Engine 23.
Power controller 24.

[0063]The input part 11 inputs the reply to a question in the case of the destination and attestation in the case of path planning. The outputting part 12 outputs the question at the time of performing the map data for course guidance, and attestation with a picture and a sound. Specifically, the outputting part 12 is provided with the indicator 121 which displays the question at the time of performing the map data for course guidance, and attestation by a picture, and the voice output part 122 which outputs the question at the time of attesting with a sound. In addition to map data required for path planning or course guidance, the storage parts store 13 stores the vehicle history information and personal information which are needed for attestation. The details of the storage parts store 13 are shown in drawing 2.

[0064]Typically, the information processing section 14 is constituted by CPU and has a function which updates the hysteresis information about the function which attests that it is a valid user besides the navigation function which the conventional car-navigation system has, and a point. The details of the information processing section 14 are shown in drawing 4. The current position primary detecting element 15 detects data required in order to compute the current position of vehicles. The current position primary detecting element 15 has the following.

GPS receiver 151.
Velocity sensor 152.
Azimuth sensor 153.
The key cylinder 211 and the cylinder key 212 are used for the car-navigation system 1

from the power supply 22 as a switch which supplies electric power. The power supply 22 supplies electric power to the car-navigation system 1 and the engine 23 of vehicles. The electric supply to the engine 23 from the power supply 22 is controlled by the power controller 24. That is, the power controller 24 answers the electric supply enabling signal from the car-navigation system 1, and starts the electric supply to the engine 23 from the power supply 22.

[0065]Drawing 2 is a block diagram showing the detailed composition of the storage parts store 13 shown in drawing 1. The storage parts store 13 is provided with the following.

Map data storage 131.

Vehicle-history-information storage 132.

Personal information storage 133.

The map data storage 131 stores map data required for the location for pinpointing a current position. The vehicle-history-information storage 132 stores the vehicle history information which is needed for attestation. In this embodiment, the vehicle-history-information storage 132 stores the entrainment date data 1322 last time showing the time which got on the spot information data table 1321 showing the hysteresis information about a point, and last time. In drawing 3, the spot information data table 1321 is shown in detail. The personal information storage 133 stores the pass word data 1331 showing the password which a user sets up beforehand.

[0066]Drawing 3 is a figure showing an example of the spot information data table 1321 shown in drawing 2. Generally, the conventional car-navigation system is the purpose of making setting out of the destination easy, and can register the position information on arbitrary points. Such a conventional car-navigation system holds the data table which stored the name of a point and the data of a position which were registered. Here, the spot information data table 1321 in the authentication device concerning this embodiment extends the data table which the conventional car-navigation system holds. Namely, the spot information data table 1321, The passage day data showing the date which resembled the spot-names data showing the name of a register point and the position data showing the position of a register point, in addition passed through the register point last time, and the passage time data showing the time which passed through the register point last time are stored for every register point, respectively. As for spot-names data, when a user registers a point, it is desirable to enable it to register the name which a user tends to memorize. Position data is referred to when updating the passage day data and passage time data of a register point. Passage day data and passage time data are used when attesting.

[0067]Drawing 4 is a block diagram showing the detailed composition of the information processing section 14. Generally, based on the information from a GPS receiver, a velocity sensor, and an azimuth sensor, the conventional car-navigation system can compute the current position of vehicles, and can perform the path planning and course guidance of the current position and destination which were computed. Such a conventional car-navigation system is provided with the following.

The location function which computes the current position of vehicles.

The path planning function to perform path planning.

The course guiding function which performs course guidance.

Here, the information processing section 14 in the authentication device concerning this

embodiment is provided with the following.
The function of the conventional car-navigation system is extended and it is the location part 141.
Path planning part 142.
It resembles the course guidance part 143, in addition is the authentication section 144.
Vehicle-history-information updating section 145.
The location part 141 computes the current position of vehicles based on the information which the current position primary detecting element 15 detects. The path planning part 142 searches for the course to arbitrary destinations based on the data of the destination outputted from the data of the current position of the vehicles computed by the location part 141, the map data memorized by the storage parts store 13, and the input part 11. The course guidance part 143 performs course guidance by displaying a course on the outputting part 12 based on the map data memorized by the information and the storage parts store 13 of the course for which it was searched by the path planning part 142. The location part 141, the path planning part 142, and the course guidance part 143 are constituted in the conventional car-navigation system as mentioned above.
[0068]The authentication section 144 performs authenticating processing, when a user takes vehicles. When the authentication section 144 attests, specifically, a reply of the user to comparison of selection of a question, spot information, and personal information and a question judges that it is a correct answer. The details of authenticating processing are shown in drawing 7 - drawing 9. The authentication section 144 transmits an electric supply enabling signal to the power controller 24, when attestation is successful. The vehicle-history-information updating section 145 performs the update process of vehicle history information. Specifically, the vehicle-history-information updating section 145 performs judgment of whether to update the spot information data table 1321, and renewal of the spot information data table 1321. The details of the update process are shown in drawing 6.
[0069]Drawing 5 is a flow chart which shows the flow of processing required for attestation in the car-navigation system 1 concerning a 1st embodiment. First, the car-navigation system 1 performs the update process of the vehicle history information used for attestation (Step S1). Specifically, the update process of vehicle history information is performed by the vehicle-history-information updating section 145 during the last vehicles entrainment. When other processings are performed in the information processing section 14, the update process of vehicle history information is a form of interruption processing, whenever the location part 141 pinpoints a current position, or is performed in the form of a subroutine call. The details of the subroutine step S1 are shown in drawing 6.
[0070]Next, the car-navigation system 1 performs authenticating processing (Step S2). Specifically, authenticating processing is performed by the authentication section 144, when a user takes vehicles. That is, a user inserts the cylinder key 212 in the key cylinder 211, and authenticating processing is started by supplying electric power to the car-navigation system 1 from the power supply 22. The details of the subroutine step S2 are shown in drawing 7 - drawing 9.
[0071]Drawing 6 is a flow chart which shows detailed processing of the subroutine step S1 of drawing 5. Here, the vehicle-history-information updating section 145 performs an update process using the coordinate data of latitude and longitude used in the car-

navigation system 1 as position data of the spot information data table 1321. Hereafter, the update process of vehicle history information is explained with reference to drawing 6.

[0072]First, the vehicle-history-information updating section 145 reads the position data showing the current position of the vehicles computed by the location part 141 (Step S11). Processing of Step S11 is performed when the location part 141 pinpoints a current position. Next, it is judged for every register point whether the current position of vehicles and the position of the vehicle-history-information updating section 145 of each register point correspond (Step S12). The judgment in Step S12 is performed by comparing with the position data about each register point of the spot information data table 1321 the position data showing the current position of the vehicles computed by the location part 141.

[0073]If the decision processing in Step S12 is explained more to details, the vehicle-history-information updating section 145 will compute the distance of the current position of vehicles, and the position of a register point first from the coordinate data showing the current position of vehicles, and the coordinate data showing the position of a register point. When the computed distance is below a predetermined value, it judges with the current position of vehicles and the position of the vehicle-history-information updating section 145 of a register point corresponding. On the other hand, when the computed distance is over the predetermined value, it judges with the current position of vehicles and the position of the vehicle-history-information updating section 145 of a register point not corresponding. Here, a predetermined value will be set as the distance (for example, 20 m) of the grade judged as the current position of vehicles and the position of a register point being in agreement, if vehicles pass through the road in front of a register point.

[0074]In the decision processing of Step S12, when the current position of vehicles and the position of a register point are in agreement, the vehicle-history-information updating section 145 updates the contents of the spot information data table 1321 (Step S13). It is carried out by rewriting the passage day data and passage time data of the spot information data table 1321 of a register point which were judged as updating in Step S13 being in agreement to the data showing a present date and time, respectively. On the other hand, when the current position of vehicles and the position of a register point are not in agreement, the vehicle-history-information updating section 145 processes Step S14, without updating the contents of the spot information data table 1321.

[0075]Next, the vehicle-history-information updating section 145 judges whether vehicles are in use. When vehicles are in use, the vehicle-history-information updating section 145 repeats processing of Step S11 - Step S13. On the other hand, when vehicles are not in use, the vehicle-history-information updating section 145 ends an update process.

[0076]Drawing 7 is a flow chart which shows detailed operation of the subroutine step S2 of drawing 5. First, the authentication section 144 judges whether the lapse period after getting on last time is less than a prescribed period (Step S21). The lapse period after getting on last time is computed from the entrainment date data 1322 and the data showing the present time last time which is stored in the vehicle-history-information storage 132. When the lapse period after getting on last time is less than a prescribed period, the authentication section 144 attests by the question about the hysteresis information about a register point (Step S22). The details of this subroutine step S22 are shown in drawing 8. Here, a prescribed period is set as the suitable period (for example, three days) which can keep in mind a passage history when a user gets on last time. As for

a prescribed period, it is desirable for the user to enable it to set up beforehand. On the other hand, when the lapse period after getting on last time exceeds a prescribed period, the authentication section 144 attests by the question about personal information (Step S23). The details of this subroutine step S23 are shown in drawing 9.

[0077]Drawing 8 is a flow chart which shows detailed operation of the subroutine step S22 of drawing 7. The authentication section 144 elects the arbitrary points of 1 from two or more register points (Step S2201). As for the election in Step S2201, it is desirable to be carried out at random using a random number etc. After a point is elected, the authentication section 144 asks [whether when it got on last time, it passed through the register point, and] a question about the elected register point using the outputting part 12 (Step S2202). The input part 11 inputs a reply of the user to a question, and outputs it to the authentication section 144. A reply form here is the alternative form of Yes or No. Next, the authentication section 144 judges whether the reply to a question is a correct answer (Step S2203). The judgment in Step S2203 is performed by comparing the entrainment date data 1322 with the data outputted from the input part 11 the passage day data about the elected register point in the spot information data table 1321 and passage time data, and last time.

[0078]When the decision processing in Step S2203 is explained more to details and the passage time about the elected register point is the back [time / entrainment] last time, When a user's reply is Yes, the authentication section 144 judges with the reply to a question being a correct answer (namely, when it is answered that it passed). Similarly, when the passage time about the elected register point is a front [time / entrainment] last time and a user's reply is No, the authentication section 144 judges with the reply to a question being a correct answer (namely, when it is answered that it has not passed). When the passage time about the elected register point is the back [time / entrainment] last time and a user's reply is No on the other hand (namely, when it answers that it has not passed), Or when the passage time about the elected register point is a front [time / entrainment] last time and a user's reply is Yes, the authentication section 144 judges with the reply to a question being a wrong solution (namely, when it is answered that it passed).

[0079]When the reply to a question is a correct answer, it is judged whether the authentication section 144 passed through the elected register point, when it got on last time (Step S2204). The judgment in Step S2204 is performed by comparing the entrainment date data 1322 with the passage day data about the elected register point in the spot information data table 1321, and passage time data last time. When the passage time about the elected register point is the back [time / entrainment] last time, the authentication section 144 asks a question about the time passed last time [of the register point elected using the outputting part 12] (Step S2205). On the other hand, when the passage time about the elected register point is a front [time / entrainment] last time, the authentication section 144 ends the question about the elected register point. A user inputs the time passed when it got on last time about the elected register point using the input part 11 to the question about the time passed last time [of the elected register point]. The authentication section 144 judges whether the reply to a question is a correct answer (Step S2206). The judgment in Step S2206 is performed by comparing the passage time data about the elected register point in the spot information data table 1321 with the data showing the time which the user inputted.

[0080]If the judgment in Step S2206 is explained more to details, the authentication

section 144 will compute first a difference with the time which passage time and a user inputted from the passage time data about the elected register point, and the data showing the time which the user inputted. Next, when a difference with the time which passage time and a user inputted is less than predetermined time, the authentication section 144 judges with the reply to a question being a correct answer. On the other hand, when the difference with the time which passage time and a user inputted is over predetermined time, the authentication section 144 judges with the reply to a question being a wrong solution. Here, predetermined time will be set as time which is judged to be a correct answer, if rough time is inputted. It is because the user generally has not memorized the passed time correctly. For example, when the time which a user inputs when predetermined time is set up in 30 minutes is within the limits of order 30 minutes from passage time, the authentication section 144 judges with the reply to a question being a correct answer.

[0081]In the decision processing of Step S2206, when the reply to the question about the elected register point is a correct answer, it is judged whether as for the authentication section 144, the number of predetermined times performed the question performed by a series of processings of Step S2201 - Step S2206 (Step S2207). When a question is asked as for the number of predetermined times, the authentication section 144 performs processing when attestation is successful (Step S2208), and ends processing.

[0082]Here, in a 1st embodiment, as processing when attestation is successful, the authentication section 144 transmits an electric supply enabling signal to the power controller 24, and updates the entrainment date data 1322 last time. By transmitting an electric supply enabling signal to the power controller 24, the electric power of the power supply 22 is supplied to the engine 23, and the engine 23 starts. Renewal of the entrainment date data 1322 is performed last time by rewriting the entrainment date data 1322 to the data showing the present time last time which is stored in the vehicle-history-information storage 132. By this, when vehicles are taken next time, entrainment time will be memorized correctly last time.

[0083]On the other hand, in the decision processing of Step S2207, when a prescribed frequency line does not require a question, the authentication section 144 repeats a series of processings of Step S2201 - Step S2206 until it asks prescribed frequency. Here, as for prescribed frequency, it is desirable to be set up in order to ask a question about two or more points for the purpose of improving the certainty of attestation, and for a user to be able to change.

[0084]Next, processing in case the reply to the question whether to have passed through the register point is a wrong solution is explained. In this case, the authentication section 144 judges whether the reply to the question whether to have passed through the register point was Yes (Step S2209). When the reply to the question whether to have passed through the register point is Yes, the authentication section 144 asks a question about the time passed last time [of the register point elected using the outputting part 12] (Step S2210). The question of Step S2210 does not have a meaning as attestation. However, the illegal use person who was a wrong solution cannot specify with which question it became a wrong solution as a question by performing the same question as the case where a reply of the user to the question whether to have passed through the register point is a correct answer. Therefore, an illegal use person's illegal use can be made difficult by forming Step S2210.

[0085]On the other hand, in the decision processing of Step S2209, when the reply to the question whether to have passed through the register point is No, the authentication section 144 does not ask a question about the time passed last time [of the elected register point]. Next, the authentication section 144 makes it indicate that attestation went wrong by the indicator 121 (Step S2211). The authentication section 144 judges to attestation whether a prescribed frequency mistake was made (Step S2212). When a prescribed frequency mistake is made at attestation, the authentication section 144 performs processing when attestation goes wrong (Step S2213), and ends processing. In a 1st embodiment, the authentication section 144 emits warning as processing when attestation goes wrong. The authentication section 144 displays a warning image on the outputting part 12, and makes a beep sound specifically output.

[0086]Drawing 9 is a flow chart which shows detailed operation of the subroutine step S23 of drawing 7. First, the authentication section 144 requires a password using the outputting part 12 (Step S2301). To a demand, the input part 11 enters the password from a user, and outputs it to the authentication section 144. The authentication section 144 judges whether an input is a correct answer (Step S2302). The judgment in Step S2302 is performed by comparing the pass word data 1331 stored in the personal information storage 133 with the data showing the password which the user entered. When an input is a correct answer, the authentication section 144 performs processing when attestation is successful (Step S2303), and ends processing. In a 1st embodiment, as processing when attestation is successful, the authentication section 144 transmits an electric supply enabling signal to the power controller 24, and updates the entrainment date data 1322 last time.

[0087]On the other hand, when an input is a wrong solution, the authentication section 144 makes it indicate that attestation went wrong by the indicator 121 in the decision processing of Step S2302 (Step S2304). The authentication section 144 judges to attestation whether a prescribed frequency mistake was made (Step S2305). When a prescribed frequency mistake is not made at attestation, the authentication section 144 redoes processing of authenticating processing from processing of Step S2301. On the other hand, when a prescribed frequency mistake is made at attestation, the authentication section 144 performs processing when attestation goes wrong (Step S2306), and ends processing. In a 1st embodiment, the authentication section 144 emits warning by the outputting part 12 as processing when attestation goes wrong.

[0088]Although the authentication device concerning this embodiment attested using the passage history about a predetermined point as vehicle history information, vehicle history information is not restricted to this. For example, when it gets on last time, it may attest, using the history of a point or the history of a course which moved as vehicle history information. It may attest using an origin and/or the destination when it gets on last time as vehicle history information. Vehicle history information may be information about speed or a VICS message receiving history of vehicles when it gets on remainder of the gasoline and last time, etc.

[0089]The authentication device concerning this embodiment attested by the question type whether to have passed through the point elected about the point which the authentication section 144 elected at random from register points when it got on last time, or about what time to have passed further when it passed. It may attest by the question type of asking the last passage time about the point which it replaced with this, and the

user itself chose arbitrary points out of the register point, and was chosen by the user. In this case, since the user should just answer passage time about the point where he has memorized the history, the burden for a user's memory is eased further.

[0090]Although the coordinate data of latitude and longitude was used for the authentication device concerning this embodiment as position data showing the position of a specified point, it may be replaced with this, and the link and/or node which are used for map data in a car-navigation system may be used for it as position data. For example, the link corresponding to the road which is in the shortest distance from a register point is memorized as position data. Since what is necessary is just to compare whether a link is in agreement in the judgment of whether the current position of vehicles and the position of a register point are in agreement according to this method, processing of a judgment becomes simple and there is an advantage that processing speed increases.

[0091]Next, a 2nd embodiment concerning this invention is described. When the theft of the key is carried out, the authentication system concerning a 2nd embodiment is a gestalt to which attestation is carried out, in order to forbid use of vehicles. Drawing 10 is a block diagram showing the composition of the authentication system concerning a 2nd embodiment. An authentication system is provided with the following in drawing 10.

The car-navigation system 3 carried in vehicles.

The key cylinder 211 and the cylinder key 212.

Power supply 22.

The engine 23, the power controller 24, and the input terminal 4 that a user holds.

The authentication system shown in drawing 10 is realizable using the component used in a 1st embodiment, and the same component. Therefore, in drawing 10, the same reference mark is given to the same component as drawing 1, and explanation is omitted.

[0092]The car-navigation system 3 is provided with the following.

Input part 11.

Outputting part 12.

Storage parts store 13.

The information processing section 14, the current position primary detecting element 15, and the communications department 16.

Thus, the car-navigation system 3 is realizable by composition with which the communications department 16 joined each component of the car-navigation system 1 concerning a 1st embodiment. The communications department 16 transmits the information inputted from the information processing section 14 to the input terminal 4.

[0093]The input terminal 4 is used in order to input the output of the question at the time of attesting, and the reply by a user. The input terminal 4 is provided with the following.

Input part 41.

Outputting part 42.

Communications department 43.

The input part 41 outputs a disable signal by a user's input. A disable signal is a signal transmitted to the car-navigation system 3, in order to forbid use of vehicles. By receiving a disable signal, the car-navigation system 3 starts the authenticating processing for forbidding use of vehicles. The input part 41 outputs the reply to the question in the case of attestation inputted by the user to the communications department 43. The outputting part 42 displays the question at the time of attesting by a picture, and outputs it with a sound. The communications department 43 communicates by radio among the

communications departments 16 of the car-navigation system 3.

[0094]Next, operation of the authentication system concerning a 2nd embodiment at the time of forbidding use of vehicles is explained. First, the input part 41 outputs a disable signal by inputting the command which forbids use of vehicles by a user. A disable signal is transmitted to the car-navigation system 3 by the communications department 43. The communications department 16 of the car-navigation system 3 receives the disable signal from the input terminal 4, and outputs to the information processing section 14. By inputting a disable signal from the communications department 16, the authentication section 144 of the information processing section 14 starts authenticating processing. That is, in a 2nd embodiment, authenticating processing is started, when the authentication section 144 receives a disable signal from the communications department 16.

[0095]The authenticating processing performed in the authentication section 144 is the same as the authenticating processing in a 1st embodiment shown in drawing 7 - drawing 9. However, it is transmitted to the input terminal 4 via the communications department 16, and the question about the attestation which the authentication section 144 performs is outputted by the outputting part 42 of the input terminal 4. A user inputs a reply to the question outputted by the outputting part 42 using the input part 41 of the input terminal 4. The reply inputted into the input part 41 is transmitted to the car-navigation system 3 via the communications department 43.

[0096]The authentication section 144 transmits an electric supply inhibiting signal to the power controller 24 as processing in Step S2303 shown in Step S2208 shown in drawing 8, and drawing 9 when attestation is successful. With an electric supply inhibiting signal, the power controller 24 forbids electric supply by the cylinder key 212 being inserted in the key cylinder 211. That is, after an electric supply inhibiting signal is transmitted from the authentication section 144, even if the cylinder key 212 is inserted in the key cylinder 211, electric supply to the engine 23 is not performed.

[0097]The authentication section 144 emits warning as processing in Step S2306 shown in Step S2213 shown in drawing 8, and drawing 9 when attestation goes wrong. Specifically, the authentication section 144 reports that attestation failed in the input terminal 4 using the communications department 16. The outputting part 42 which received the notice via the communications department 43 displays a warning image, and outputs a beep sound.

[0098]By the above operation, the authentication system concerning a 2nd embodiment forbids use of the vehicles by the cylinder key 212. When canceling prohibition of use of vehicles, the same attestation as the above is performed. First, the input part 41 outputs a prohibition release signal by inputting the command of which prohibition of use of vehicles is canceled by a user. It is transmitted to the car-navigation system 3, and a prohibition release signal is inputted into the authentication section 144. Thereby, the authentication section 144 of the information processing section 14 starts authenticating processing. When attestation is successful, the authentication section 144 transmits a release signal to the power controller 24. With a release signal, the power controller 24 cancels prohibition of electric supply by the cylinder key 212 being inserted in the key cylinder 211. That is, if the cylinder key 212 is inserted in the key cylinder 211 after a release signal is transmitted from the authentication section 144, electric supply to the engine 23 will be

performed.

[0099]The authentication system concerning a 2nd embodiment can use vehicles by attestation which used vehicle history information. First, the input part 41 outputs a beginning-of-using signal by inputting the command which uses vehicles by a user. It is transmitted to the car-navigation system 3, and a beginning-of-using signal is inputted into the authentication section 144. Thereby, the authentication section 144 of the information processing section 14 starts authenticating processing. When attestation is successful, the authentication section 144 transmits an electric supply enabling signal to the power controller 24. The power controller 24 starts the electric supply to the engine 23 from the power supply 22 to an electric supply enabling signal. The power controller 24 gives priority to the electric supply enabling signal from the authentication section 144 to the electric supply inhibiting signal from the authentication section 144. It is possible to use vehicles by attestation of an authentication system by this, even if it is an electric supply prohibited state.

[0100]In a 2nd embodiment, attestation which used the key is performed in the case of usual entrainment. That is, the power controller 24 starts the electric supply to the engine 23 from the power supply 22 by inserting the cylinder key 212 in the key cylinder 211. In this case, authenticating processing by the authentication section 144 of the information processing section 14 is not performed. The attestation using a key may attest by including specific electronic intelligence in a key typically like an immobilizer besides what attests with the shape of a key as mentioned above.

[0101]In a 2nd embodiment, in order to perform the question and reply in the case of authenticating processing, the input terminal 4 is used. This takes into consideration the case where the cylinder key 212 is needed, in order to open the door of vehicles. In other embodiments, it may be a gestalt for which the input part 11 and the outputting part 12 of the car-navigation system 3 are used. The communication between the communications department 16 of the car-navigation system 3 and the communications department 43 of the input terminal 4 is not restricted to this, for example, although it is realizable by Bluetooth.

[0102]Next, a 3rd embodiment concerning this invention is described. The authentication system concerning a 3rd embodiment is a gestalt for which attestation by vehicle history information is used as one of two or more authentication methods used in an authentication system. Drawing 11 is a block diagram showing the composition of the authentication system concerning a 3rd embodiment. An authentication system is provided with the following in drawing 11.

Car-navigation system 5.

The key cylinder 211 and the cylinder key 212.

Power supply 22.

The engine 23, the power controller 24, the authenticating processing control device 25, and the communication device 26.

The authenticating processing control device 25 controls the processing performed when attested with it being a valid user about each authentication method. The details of operation of the authenticating processing control device 25 are shown in drawing 12. The communication device 26 notifies that vehicles are used to the user. The authentication system shown in drawing 11 is realizable using the component used in a 1st embodiment, and the same component. Therefore, in drawing 11, the same reference mark is given to

the same component as drawing 1, and explanation is omitted.

[0103]Next, operation of the authentication system concerning a 3rd embodiment is explained. Drawing 12 is a figure showing the relation between the authentication method used in the authentication system shown in drawing 11, and the processing to an authentication result. In the authentication system concerning a 3rd embodiment, the authentication method using the cylinder key 212 and the authentication method using vehicle history information are used. Like drawing 12, when attestation by the cylinder key 212 goes wrong, the authenticating processing control device 25 presupposes that use of vehicles is impossible. The authenticating processing control device 25 performs report processing in this case. When the attestation using the cylinder key 212 is successful and the attestation using vehicle history information goes wrong, the authenticating processing control device 25 makes vehicles usable, and performs report processing. For example, report processing is made, even when the theft of the cylinder key 212 is carried out and vehicles are used unjustly. When the attestation using the cylinder key 212 is successful and the attestation using vehicle history information is successful, the authenticating processing control device 25 makes vehicles usable, and does not perform report processing. Hereafter, the details of processing of the authenticating processing control device 25 are explained.

[0104]Drawing 13 is a flow chart which shows the flow of the processing in the authenticating processing control device 25 shown in drawing 11. The processing in the authenticating processing control device 25 is started by inserting the cylinder key 212 in the key cylinder 211. First, the authenticating processing control device 25 performs attestation by a key (Step S31). Here, the attestation by a key attests by including specific electronic intelligence in the cylinder key 212 typically like an immobilizer. The method of attestation by a key may attest [whether for example, the shape of the mechanical cylinder key 212 agrees in the key cylinder 211, and] not only in the above.

[0105]Next, the authenticating processing control device 25 judges whether the attestation in Step S31 was successful (Step S32). When the attestation in Step S31 goes wrong, the authenticating processing control device 25 forbids use of vehicles (Step S33). Specifically, the authenticating processing control device 25 does not transmit an electric supply enabling signal to the power controller 24. Therefore, since electric supply is not performed from the power supply 22, the engine 23 is not put into operation. The authenticating processing control device 25 performs report processing (Step S34), and ends processing. Report processing of Step S34 is performed when the authenticating processing control device 25 transmits a communication signal to the communication device 26. With a communication signal, the communication device 26 notifies that there is a possibility that vehicles may be unjustly used to the user. Specifically, the communication device 26 notifies that vehicles are used to the communication terminal which the user who does not illustrate has. As long as it does not restrict the method of the report by the communication device 26 above and notifies it to a user, it may be what kind of composition.

[0106]On the other hand, in the decision processing of Step S32, when the attestation in Step S31 is successful, the authenticating processing control device 25 permits use of vehicles (Step S35). Processing of Step S35 is performed when the authenticating processing control device 25 transmits an electric supply enabling signal to the power

controller 24. Answering an electric supply enabling signal, the power controller 24 starts the electric supply to the engine 23 from the power supply 22.

[0107]After permitting use of vehicles, the authenticating processing control device 25 requires the start of the authenticating processing using vehicle history information from the car-navigation system 5 (Step S36). Specifically, the authenticating processing control device 25 transmits an attestation start signal to the information processing section 14 of the car-navigation system 5. With an attestation start signal, the authentication section 144 of the information processing section 14 starts authenticating processing. Here, the authenticating processing by the authentication section 144 is the same as the authenticating processing shown in drawing 7 - drawing 9. The authentication section 144 reports that attestation was successful to the authenticating processing control device 25 as processing when the attestation in Step S2303 shown in Step S2208 shown in drawing 8 and drawing 9 is successful. The authentication section 144 reports that attestation went wrong to the authenticating processing control device 25 as processing in Step S2306 shown in Step S2213 shown in drawing 8, and drawing 9 on the other hand when attestation goes wrong.

[0108]The authenticating processing control device 25 judges whether the attestation by vehicle history information was successful after Step S36 (Step S37). Decision processing in Step S37 is performed by whether the notice of the purport that attestation was successful was received from the authentication section 144. In the decision processing in Step S37, when judged with the attestation by vehicle history information having gone wrong, the authenticating processing control device 25 processes Step S34, and ends processing. On the other hand, when judged with the attestation by vehicle history information having been successful, the authenticating processing control device 25 ends processing.

[0109]Next, a 4th embodiment concerning this invention is described. The authentication system concerning a 4th embodiment is a gestalt which performs attestation which used vehicle history information using the terminal which a user has. Drawing 14 is a block diagram showing the composition of the authentication system concerning a 4th embodiment. An authentication system is provided with the following in drawing 14.

The car-navigation system 6 carried in vehicles.

The key cylinder 211 and the cylinder key 212.

Power supply 22.

The engine 23, the power controller 24, and the authentication terminal 7.

The authentication system shown in drawing 14 is realizable using the component used in a 1st embodiment, and the same component. Therefore, in drawing 14, the same reference mark is given to the same component as drawing 1, and explanation is omitted.

[0110]The car-navigation system 6 is provided with the following.

Input part 11.

Outputting part 12.

Storage parts store 13.

The information processing section 14, the current position primary detecting element 15, and the communications department 66.

Thus, the car-navigation system 6 is the composition that the communications department 66 joined each component of the car-navigation system 1 concerning a 1st embodiment.

The communications department 66 transmits and receives data among the communications departments 75 of the authentication terminal 7.
[0111]The authentication terminal 7 is provided with the following.
Input part 71.
Outputting part 72.
The storage parts store 73, the authentication processing part 74.
Communications department 75.
The input part 71 is used in order to input the reply to a question in the case of a user's attestation. The outputting part 72 outputs the question at the time of attesting with a picture and a sound. The storage parts store 73 stores the vehicle history information and personal information which are needed for attestation. The authentication processing part 74 performs authenticating processing which used vehicle history information. The communications department 75 communicates by radio among the communications departments 66 of the car-navigation system 6.
[0112]Drawing 15 is a flow chart which shows the flow of processing required for attestation in the authentication terminal 7 shown in drawing 14. First, the authentication terminal 7 acquires the vehicle history information used for attestation from the car-navigation system 6 (step S4). Processing of step S4 is performed by transmitting the vehicle history information memorized by the storage parts store 13 of the car-navigation system 6 to the authentication terminal 7, when use of vehicles is completed. More specifically, the information processing section 14 transmits the vehicle history information memorized by the storage parts store 13 to the authentication terminal 7 via the communications department 66, when the engine of vehicles is come by off. Vehicle history information is memorized by the storage parts store 73 of the authentication terminal 7 by the above. The timing which processes step S4 may be, just before authenticating processing is performed by the authentication terminal 7 not only in the above-mentioned timing, for example.
[0113]After acquiring vehicle history information, the authentication terminal 7 performs authenticating processing (Step S5). In the authentication processing part 74, the authenticating processing of Step S5 is started, when a command of an attestation start is inputted by the user using the input part 71. Here, the authenticating processing of Step S5 is the same as the authenticating processing of the authentication section 144 concerning a 1st embodiment shown in drawing 7 - drawing 9. The authentication processing part 74 reports that attestation was successful to the car-navigation system 6 as processing when the attestation in Step S2303 shown in Step S2208 shown in drawing 8 and drawing 9 is successful. Typically in the notice of the purport that the attestation to the navigation system 6 from the authentication terminal 7 was successful, attestation, an electronic signature, or encryption is performed. Thereby, the unjust operation from the outside is made not to be performed.
[0114]The information processing section 14 of the car-navigation system 6 which received the notice of the purport that attestation was successful transmits an electric supply inhibiting signal to the power controller 24. With an electric supply inhibiting signal, the power controller 24 forbids electric supply by the cylinder key 212 being inserted in the key cylinder 211. That is, after electric supply inhibiting-signal transmitting from the authentication section 144, even if the cylinder key 212 is inserted in the key

cylinder 211, electric supply to the engine 23 is not performed. The power controller 24 gives priority to the electric supply enabling signal from the authentication section 144 to the electric supply inhibiting signal from the authentication section 144. It is possible to use vehicles by attestation of an authentication system by this, even if it is an electric supply prohibited state.

[0115]The authentication section 144 emits warning as processing in Step S2306 shown in Step S2213 shown in drawing 8, and drawing 9 when attestation goes wrong. Specifically, the authentication section 144 reports that attestation went wrong to the authentication terminal 7 using the communications department 66. The authentication processing part 74 which received the notice via the communications department 75 displays a warning image on the outputting part 42, and makes a beep sound output.

[0116]As mentioned above, in a 4th embodiment, when forbidding use of vehicles, the authentication terminal 7 is used. Here, in other embodiments, the authentication terminal 7 may be the composition of being used when using vehicles. Therefore, also in a 1st embodiment, the authentication terminal 7 used in the authentication system concerning a 4th embodiment can be used. In this case, the user attests beforehand out of the car with the authentication terminal 7, and can be prevented from performing attestation troublesome at the time of vehicles entrainment.

[0117]In a 4th embodiment, attestation in the authentication terminal 7 is performed in order to use vehicles, or in order to forbid use of vehicles. Here, in other embodiments, the use of the authentication terminal 7 is not restricted to the thing about use of vehicles. For example, when the authentication terminal 7 is what has a clearing function of a fee and charge settlement is performed, attestation of being a valid user is performed. In this case, in order to attest a valid user, the attestation which used vehicle history information can be used.

[0118]The power controller 24 of a 1st embodiment, a 2nd embodiment, a 3rd embodiment, and each 4th embodiment does not necessarily need to be a device which restricts the electric power supply to an engine. The power controller 24 should just be the method of controlling use of vehicles, or a device.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the composition of the vehicles carrying the authentication device concerning one embodiment of this invention.
[Drawing 2]It is a block diagram showing the detailed composition of the storage parts store 3 shown in drawing 1.
[Drawing 3]It is a figure showing an example of the spot information data table 1321 stored in the vehicle-history-information storage 132 shown in drawing 2.
[Drawing 4]It is a block diagram showing the detailed composition of the information processing section 4 shown in drawing 1.
[Drawing 5]It is a flow chart which shows the flow of processing required for attestation in the car-navigation system 1 concerning a 1st embodiment.
[Drawing 6]It is a flow chart which shows detailed processing of the subroutine step S1 of drawing 5.
[Drawing 7]It is a flow chart which shows detailed operation of the subroutine step S2 of drawing 5.
[Drawing 8]It is a flow chart which shows detailed operation of the subroutine step S22 of drawing 7.
[Drawing 9]It is a flow chart which shows detailed operation of the subroutine step S23 of drawing 7.
[Drawing 10]It is a block diagram showing the composition of the authentication system concerning a 2nd embodiment.
[Drawing 11]It is a block diagram showing the composition of the authentication system concerning a 3rd embodiment.
[Drawing 12]It is a figure showing the relation between the authentication method used in the authentication system shown in drawing 11, and the processing to each authentication result.
[Drawing 13]It is a flow chart which shows the flow of the control management in the authenticating processing control device 25 shown in drawing 11.
[Drawing 14]It is a block diagram showing the composition of the authentication system concerning a 4th embodiment.
[Drawing 15]It is a flow chart which shows the flow of processing required for attestation

in the authentication terminal 7 shown in drawing 14.

[Description of Notations]

1, 3, 5, 6 -- Car-navigation system
4 -- Input terminal
7 -- Authentication terminal
11, 41, 71 -- Input part
12, 42, 72 -- Outputting part
13, 73 -- Storage parts store
14 -- Information processing section
15 -- Current position primary detecting element
16, 43, 66, 75 -- Communications department
22 -- Power supply
23 -- Engine
24 -- Power controller
25 -- Authenticating processing control device
26 -- Communication device
74 -- Authentication processing part
121 -- Indicator
122 -- Voice output part
131 -- Map data storage
132 -- Vehicle-history-information storage
133 -- Personal information storage
141 -- Location part
142 -- Path planning part
143 -- Course guidance part
144 -- Authentication section
145 -- Vehicle-history-information updating section
151 -- GPS receiver
152 -- Velocity sensor
153 -- Azimuth sensor
211 -- Key cylinder
212 -- Cylinder key
1321 -- Spot information data table
1322 -- Last entrainment date data
1331 -- Pass word data

[Translation done.]

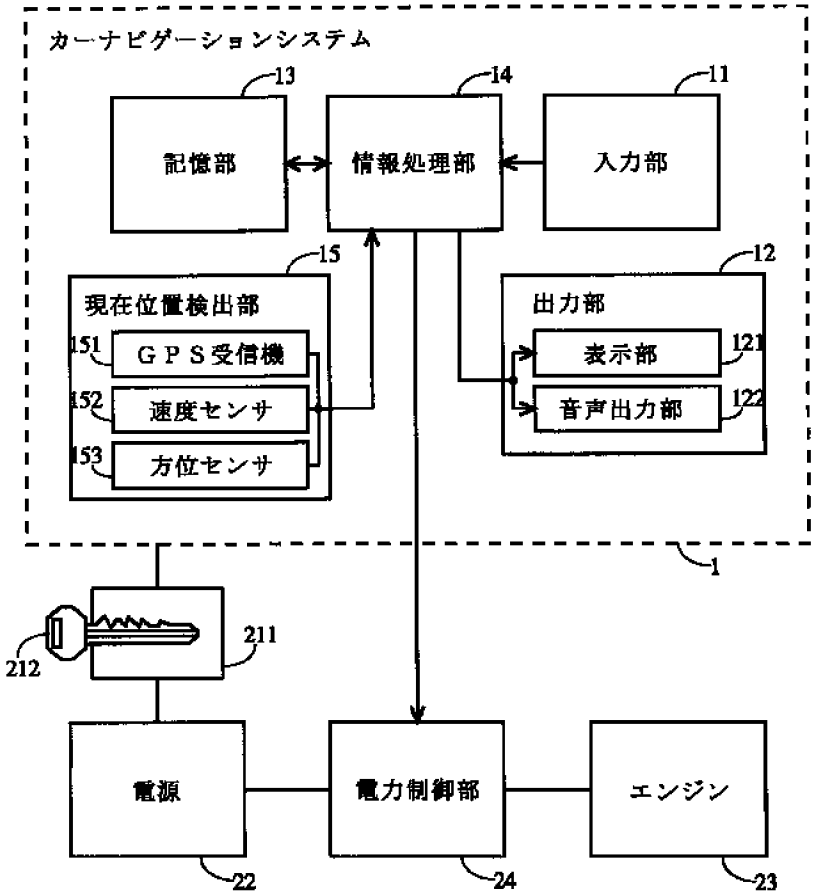
* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

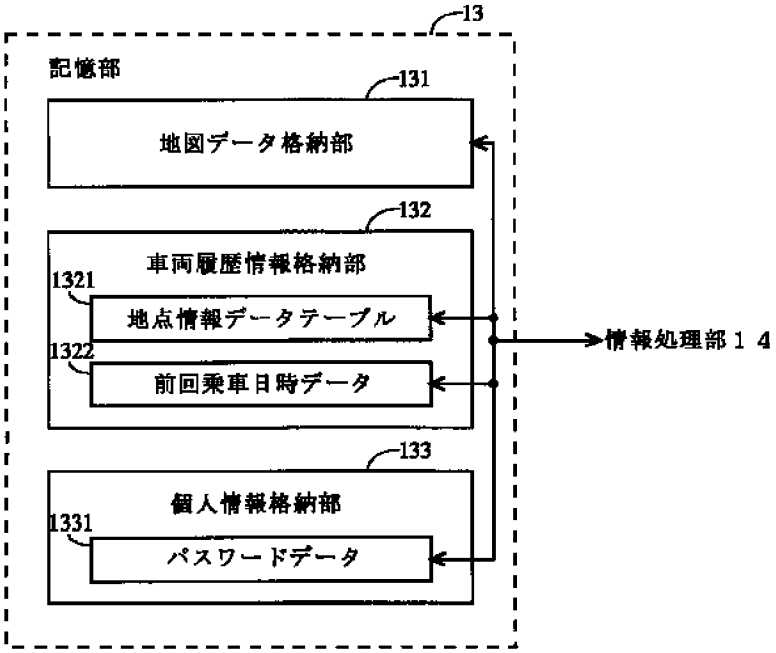
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]



[Drawing 2]

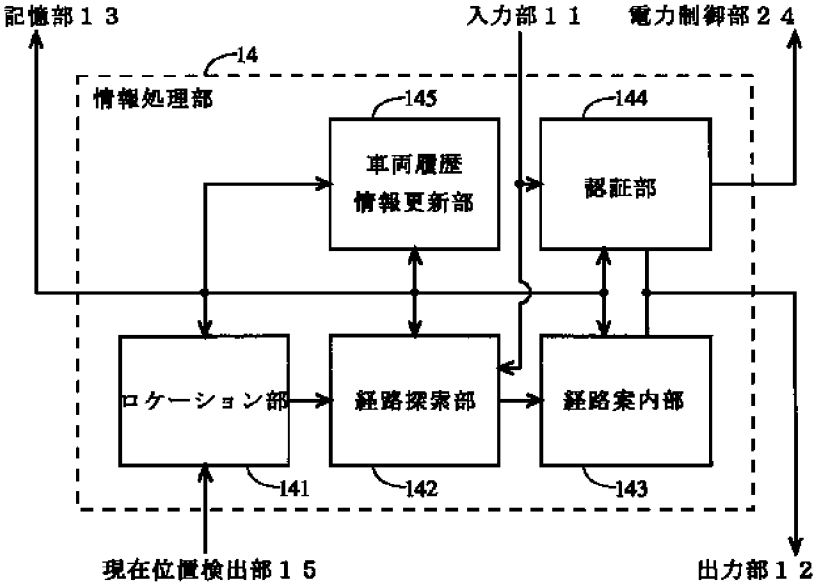


[Drawing 3]

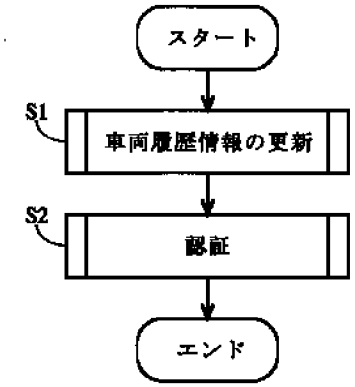
1321

地点名	位置	通過日	通過時刻
○○駅	緯度・経度	００．１０．１３	１３：２５
○○橋	緯度・経度	００．０９．２８	２０：３８
○○交差点	緯度・経度	００．１０．１２	０９：１５
○○銀行	緯度・経度	００．１０．２１	１２：４０
・	・	・	・
・	・	・	・
・	・	・	・

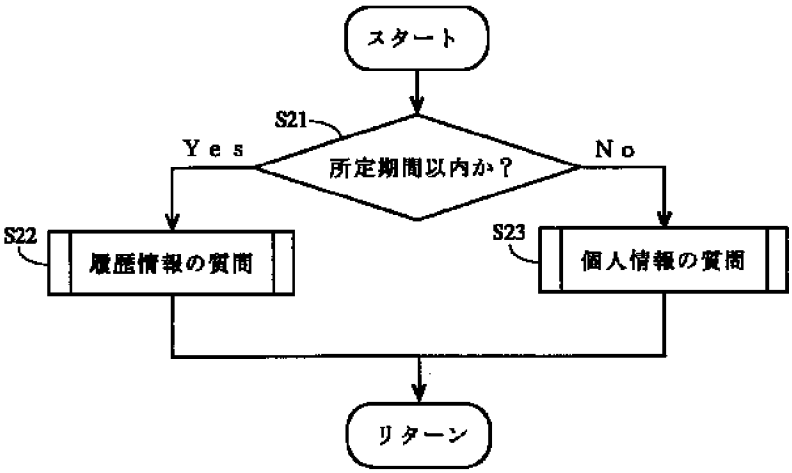
[Drawing 4]



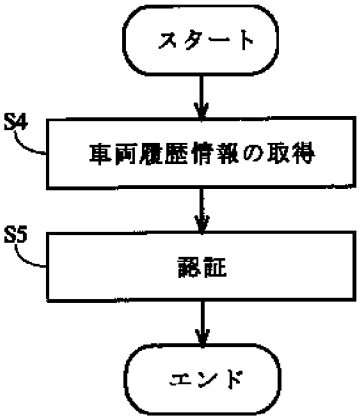
[Drawing 5]



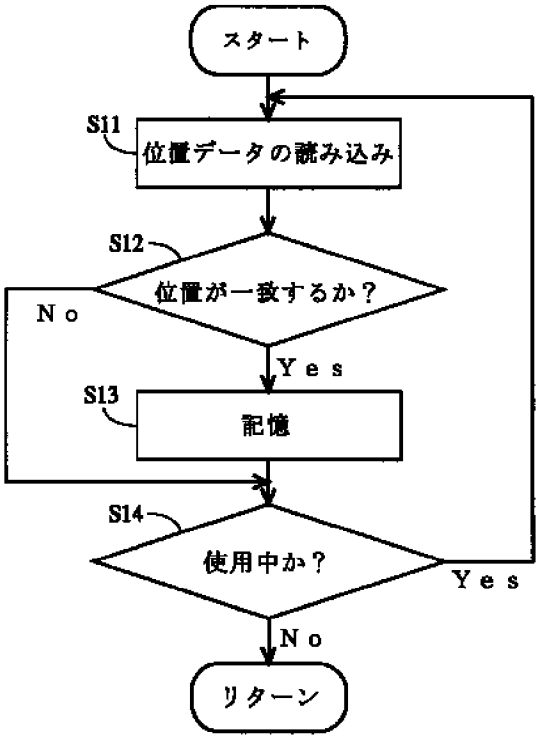
[Drawing 7]



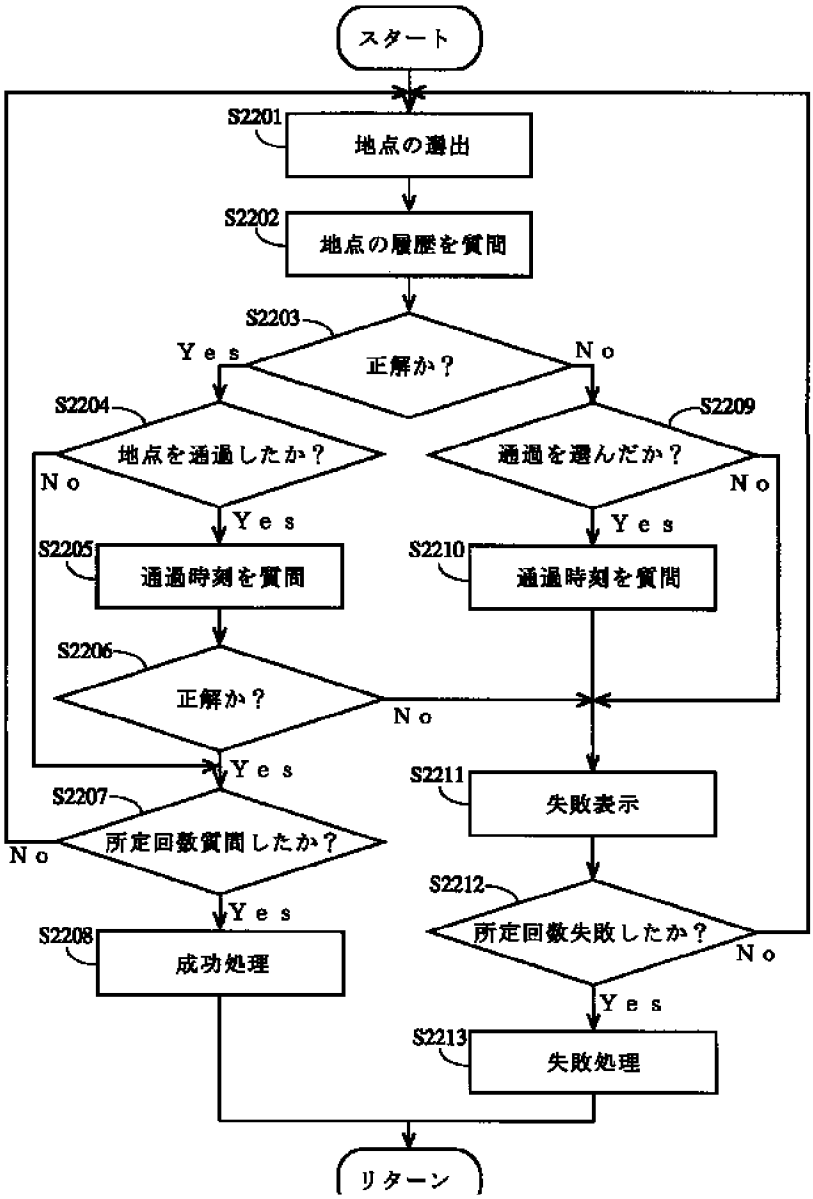
[Drawing 15]

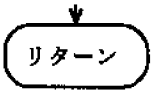


[Drawing 6]

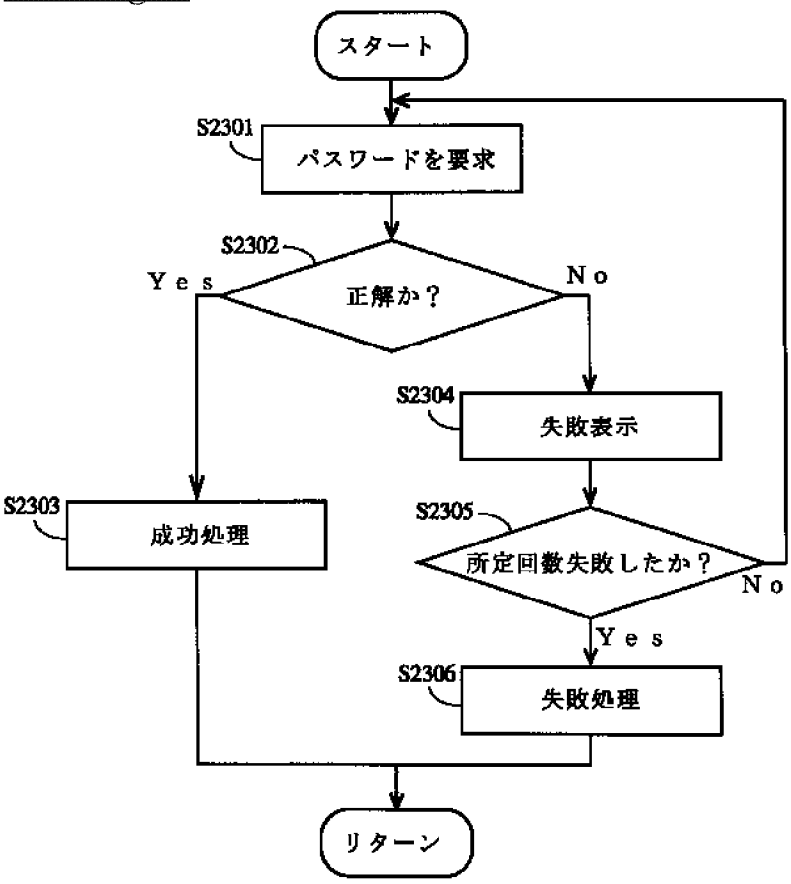

スタート
S11
位置データの読み込み
S12
位置が一致するか？
No
Yes
S13
記憶
S14
使用中か？
Yes
No
リターン

[Drawing 8]

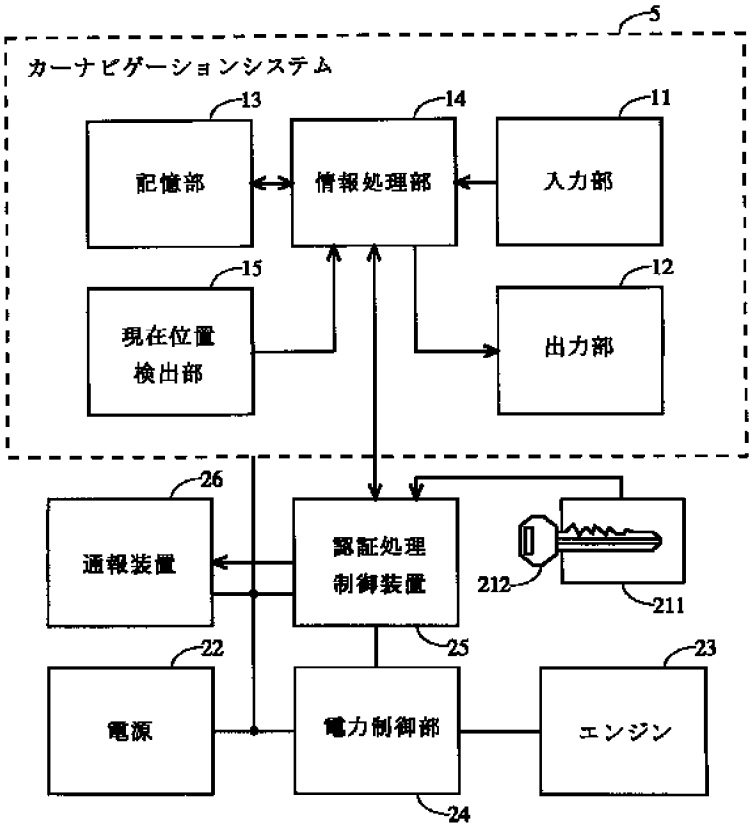

スタート
S2201
地点の選出
S2202
地点の履歴を質問
S2203
正解か？
Yes
No
S2204
地点を通過したか？
No
Yes
S2205
通過時刻を質問
S2206
正解か？
No
Yes
S2207
所定回数質問したか？
No
Yes
S2208
成功処理
S2209
通過を選んだか？
No
Yes
S2210
通過時刻を質問
S2211
失敗表示
S2212
所定回数失敗したか？
No
Yes
S2213
失敗処理
リターン



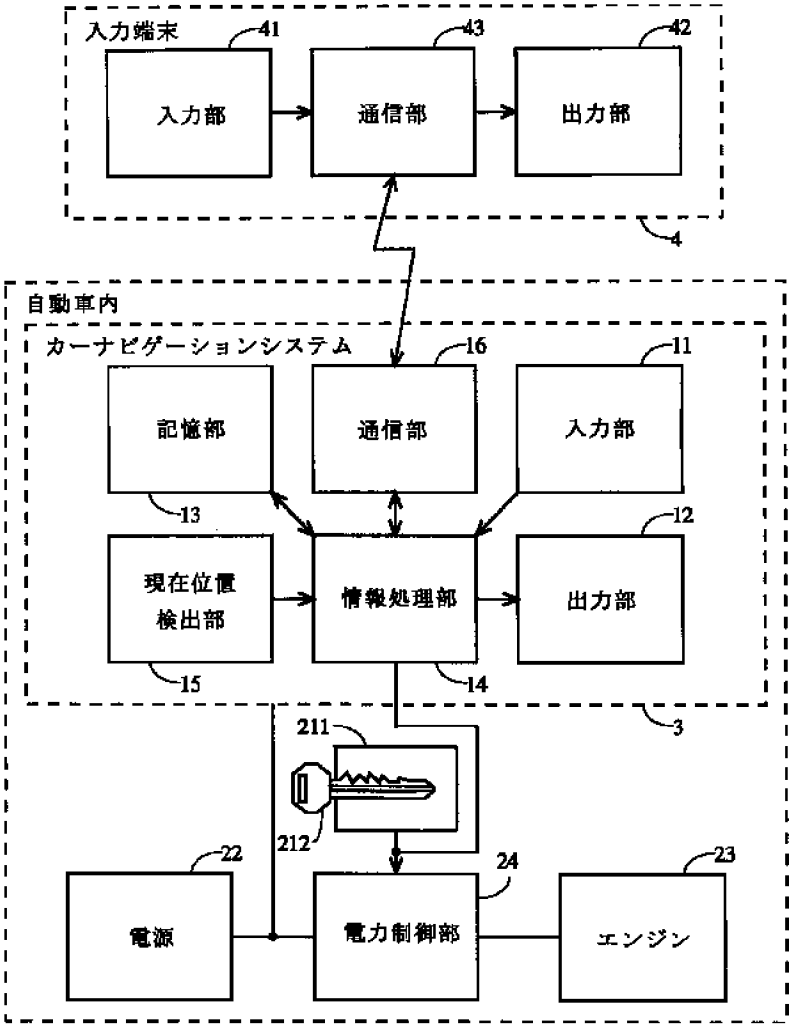
[Drawing 9]



[Drawing 11]



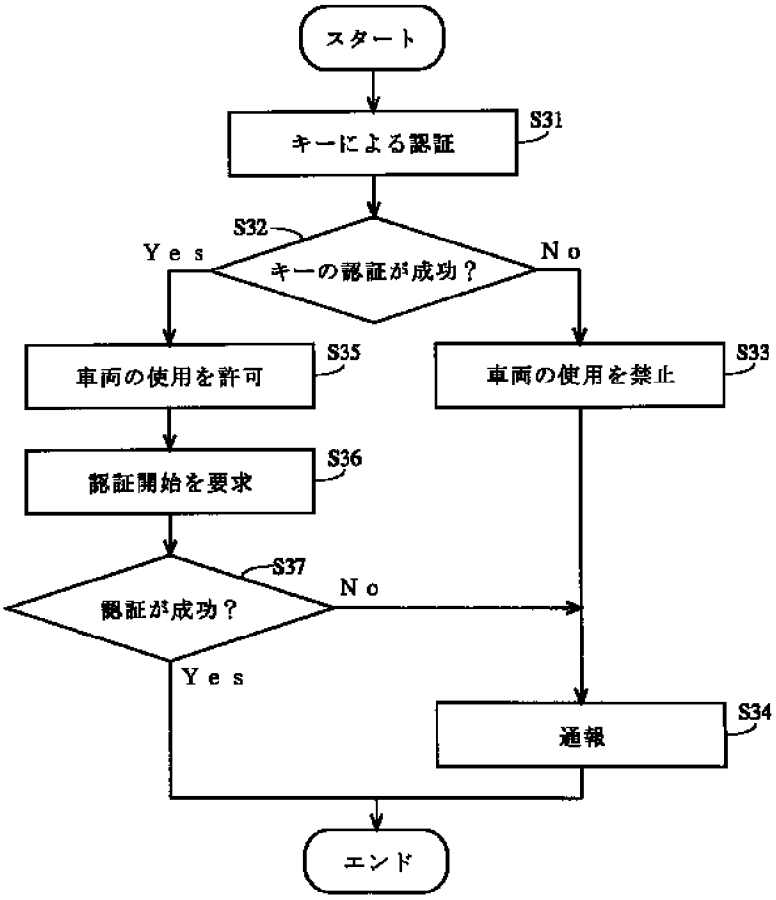
[Drawing 10]



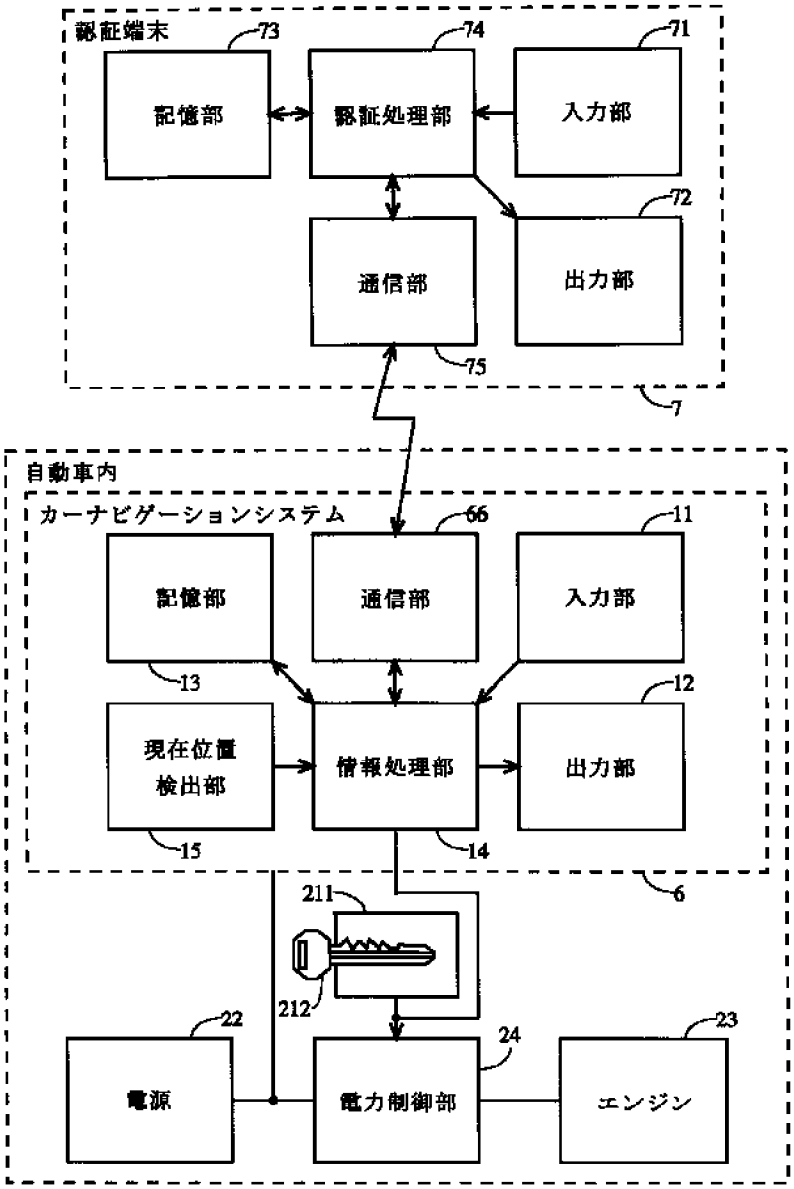
[Drawing 12]

		車両履歴情報による認証	
		成功	失敗
キーによる認証	成功	・車両使用可 ・通報不要	・車両使用可 ・通報要
	失敗	・車両使用不可 ・通報要	

[Drawing 13]


スタート
キーによる認証
S31
S32
Yes
キーの認証が成功？
No
車両の使用を許可
S35
車両の使用を禁止
S33
認証開始を要求
S36
S37
認証が成功？
No
Yes
通報
S34
エンド

[Drawing 14]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－211358
（P2002－211358A）
(43)公開日　平成14年７月31日(2002.7.31)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｂ６０Ｒ　25/04	６０２	Ｂ６０Ｒ　25/04	６０２	２Ｆ０２９
	６１０		６１０	５Ｊ１０４
25/10	６１８	25/10	６１８	
Ｇ０１Ｃ　21/00		Ｇ０１Ｃ　21/00	Ａ	
// Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ	

審査請求　未請求　請求項の数23　ＯＬ　（全 20 頁）　最終頁に続く

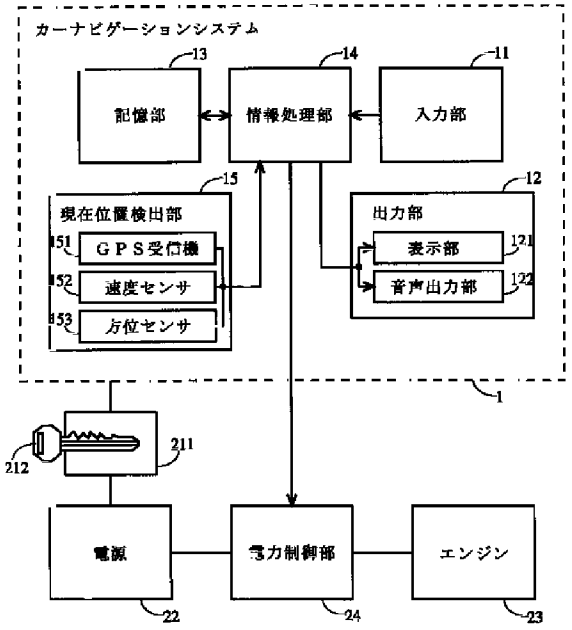
(21)出願番号　特願2001－270924(P2001－270924)
(22)出願日　平成13年９月６日(2001.9.6)
(31)優先権主張番号　特願2000－349875(P2000－349875)
(32)優先日　平成12年11月16日(2000.11.16)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　阿多　輝明
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　阪本　清美
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100098291
弁理士　小笠原　史朗

最終頁に続く

(54)【発明の名称】　認証装置および認証方法

(57)【要約】
【課題】　今までにない認証の方法により、小型化および低コスト化が可能で、かつ、安全性の高い、車両を操作した正当なユーザを認証する認証装置を提供することである。
【解決手段】　現在位置検出部１５は、車両の使用に伴い変化する車両履歴情報を検出し、記憶部１３は車両履歴情報を格納しておく。認証の際には、出力部１２は車両履歴情報についての質問を行い、ユーザは入力部１１により質問に対する回答を入力する。情報処理部１４は記憶部１３に格納される車両履歴情報とユーザの回答に基づき、質問が正解であるかどうかを判定することにより、車両の正当なユーザの認証を行う。



【特許請求の範囲】
【請求項１】　車両の正当なユーザの認証を行うための認証装置であって、
前記車両の使用に伴い変化する車両履歴情報を検出する車両履歴情報検出部と、
前記車両履歴情報検出部により検出された車両履歴情報を格納する車両履歴情報格納部と、
前記車両履歴情報についての質問を出力する出力部と、
前記車両履歴情報についての質問に対するユーザの回答を入力する回答入力部と、
前記車両履歴情報格納部に格納されている車両履歴情報と前記ユーザの回答とに基づき、正当なユーザであることを認証するユーザ認証部とを備える、認証装置。
【請求項２】　前記車両履歴情報は、１以上の所定地点についての履歴を表す地点履歴情報を含む、請求項１に記載の認証装置。
【請求項３】　前記地点履歴情報は、前記ユーザにより予め登録された１以上の登録地点について、前記登録地点を前回通過した日時と、前記車両に前回乗車した日時とについての情報を含む、請求項２に記載の認証装置。
【請求項４】　前記ユーザ認証部は、前記登録地点から任意の地点を選出し、
前記出力部は、前記ユーザ認証部により選出された地点について、前記車両に前回乗車したときに通過したかどうかの質問と、前記車両に前回乗車したときに通過した場合は、前記車両に前回乗車したときに通過した時刻の質問とを出力することを特徴とする、請求項３に記載の認証装置。
【請求項５】　前記回答入力部は、前記登録地点のうち前記ユーザにより選択された地点を入力し、
前記出力部は、前記回答入力部において入力された地点について、前記車両に前回乗車したときに通過した時刻の質問を出力することを特徴とする、請求項３に記載の認証装置。
【請求項６】　前記ユーザに関する固有の情報および／または前記ユーザにより予め設定されるパスワードを含む個人情報を格納する個人情報格納部をさらに備え、
前記出力部は、
前記車両に前回乗車してからの経過期間が所定期間以内である場合は、前記車両履歴情報についての質問を出力し、
前記経過期間が前記所定期間を越える場合は、前記個人情報についての質問を出力し、
前記回答入力部は、
前記経過期間が前記所定期間以内である場合は、前記車両履歴情報についての質問に対するユーザの回答を入力し、
前記経過期間が前記所定期間を越える場合は、前記個人情報についての質問に対するユーザの回答を入力し、
前記ユーザ認証部は、
前記経過期間が前記所定期間以内である場合は、前記車両履歴情報と前記ユーザの回答とに基づき、正当なユーザであるかどうかを判定し、
前記経過期間が前記所定期間を越える場合は、前記個人情報と前記ユーザの回答とに基づき、正当なユーザであることを認証することを特徴とする、請求項１に記載の認証装置。
【請求項７】　車両のエンジンへの給電を行う電力制御部をさらに備え、
前記ユーザ認証部は、正当なユーザであることを認証した場合、前記電力制御部に給電を開始させることを特徴とする、請求項１に記載の認証装置。
【請求項８】　車両のエンジンへの給電を行う電力制御部と、
キーを用いた認証を行い、正規のキーであることを認証した場合、前記電力制御部に給電を開始させるキー認証部と、
前記車両の使用制限命令を入力する制限命令入力部とをさらに備え、
前記ユーザ認証部は、前記車両の使用制限命令に応じて認証を行い、正当なユーザであると認証した場合、前記キー認証部によって前記電力制御部が給電を開始することを禁止することを特徴とする、請求項１に記載の認証装置。
【請求項９】　前記車両の使用命令を入力する使用命令入力部をさらに備え、
前記ユーザ認証部は、前記車両の使用命令に応じて認証を行い、正当なユーザであると認証した場合、前記電力制御部に給電を開始させることを特徴とする、請求項８に記載の認証装置。
【請求項１０】　車両のエンジンへの給電を行う電力制御部と、
キーを用いた認証を行い、正規のキーであることを認証した場合、前記電力制御部に対して給電を開始させるキー認証部と、
前記電力制御部による給電が開始されてから所定時間内に、前記ユーザ認証部が正当なユーザであることを認証しなかった場合、車両が不正に使用されていることをユーザに通報する通報部とをさらに備える、請求項１に記載の認証装置。
【請求項１１】　カーナビゲーションシステムの一部として構成されたことを特徴とする、請求項１に記載の認証装置。
【請求項１２】　車両の使用に伴い変化する車両履歴情報についての質問の出力および当該質問に対するユーザの回答の入力を行う入力端末と通信可能な認証装置であって、
前記車両履歴情報を検出する車両履歴情報検出部と、
前記車両履歴情報検出部により検出された車両履歴情報を格納する車両履歴情報格納部と、

前記車両履歴情報についての質問を前記入力端末に送信し、当該質問に対するユーザの回答を当該入力端末から受信する通信部と、
前記車両履歴情報格納部に格納されている車両履歴情報と前記ユーザの回答とに基づき、正当なユーザであることを認証するユーザ認証部とを備える、認証装置。
【請求項１３】　車両に搭載され、当該車両の正当なユーザの認証を行う認証装置と、当該認証装置と通信可能な入力端末とを含む認証システムであって、
前記認証装置は、
前記車両の使用に伴い変化する車両履歴情報を検出する車両履歴情報検出部と、
前記車両履歴情報検出部により検出された車両履歴情報を格納する車両履歴情報格納部と、
前記車両履歴情報についての質問を前記入力端末に対して送信し、当該質問に対するユーザの回答を当該入力端末から受信する通信部と、
前記車両履歴情報格納部に格納されている車両履歴情報と前記ユーザの回答とに基づき、正当なユーザであることを認証するユーザ認証部とを備え、
前記入力端末は、
前記認証装置から送信されてくる前記車両履歴情報についての質問を出力する端末側出力部と、
前記車両履歴情報についての質問に対するユーザの回答を入力する端末側回答入力部と、
前記ユーザの回答を前記認証装置に送信する端末側通信部とを備える、認証システム。
【請求項１４】　前記認証装置は、
車両のエンジンへの給電を行う電力制御部と、
キーを用いた認証を行い、正規のキーであることを認証した場合、前記電力制御部に対して給電を開始させるキー認証部とをさらに備え、
前記入力端末は、前記車両の使用制限命令を入力する端末側制限命令入力部をさらに備え、
前記ユーザ認証部は、前記車両の使用制限命令に応じて認証を行い、正当なユーザであると認証した場合、前記キー認証部によって前記電力制御部が給電を開始することを禁止することを特徴とする、請求項１３に記載の認証システム。
【請求項１５】　前記入力端末は、前記車両の使用命令を入力する端末側使用命令入力部をさらに備え、
前記ユーザ認証部は、前記車両の使用命令に応じて認証を行い、正当なユーザであると認証した場合、前記電力制御部に給電を開始させることを特徴とする、請求項１４に記載の認証システム。
【請求項１６】　車両に搭載される車両側装置と、当該車両側装置と通信可能な認証端末とを含む認証システムであって、
前記車両側装置は、
前記車両の使用に伴い変化する車両履歴情報を検出する車両履歴情報検出部と、
前記車両履歴情報検出部により検出された車両履歴情報を前記認証端末に対して送信する通信部とを備え、
前記認証端末は、
前記通信部から送信されてくる車両履歴情報を格納する端末側車両履歴情報格納部と、
前記車両履歴情報についての質問を出力する端末側出力部と、
前記車両履歴情報についての質問に対するユーザの回答を入力する端末側回答入力部と、
前記端末側車両履歴情報格納部に格納されている車両履歴情報と前記ユーザの回答とに基づき、正当なユーザであることを認証する端末側ユーザ認証部とを備える、認証システム。
【請求項１７】　前記認証端末は、前記端末側ユーザ認証部による認証結果を、前記車両側装置に対して送信する端末側通信部をさらに備え、
前記車両側装置は、前記端末側通信部から受信した認証結果に基づいて、前記車両の盗難を防止するための処理を行う盗難防止処理部をさらに備える、請求項１６に記載の認証システム。
【請求項１８】　前記盗難防止処理部は、車両のエンジンへの給電を行う電力制御部を含み、
前記車両側装置は、キーを用いた認証を行い、正規のキーであることを認証した場合、前記電力制御部に対して給電を開始させるキー認証部をさらに備え、
前記認証端末は、前記車両の使用制限命令を入力する端末側制限命令入力部をさらに備え、
前記端末側ユーザ認証部は、前記車両の使用制限命令に応じて認証を行い、正当なユーザであると認証した場合、前記端末側通信部に前記電力制御部に対して給電禁止信号を送信させ、それによって、前記キー認証部によって前記電力制御部が給電を開始することを禁止することを特徴とする、請求項１７に記載の認証システム。
【請求項１９】　前記認証端末は、前記車両の使用命令を入力する端末側使用命令入力部をさらに備え、
前記端末側ユーザ認証部は、前記車両の使用命令に応じて認証を行い、正当なユーザであると認証した場合、前記端末側通信部に前記電力制御部に対して給電信号を送信させ、それによって、前記電力制御部に給電を開始させることを特徴とする、請求項１８に記載の認証システム。
【請求項２０】　前記車両側装置は、前記車両履歴情報検出部により検出された車両履歴情報を格納する車両履歴情報格納部をさらに備え、
前記通信部は、車両の使用が終了したとき、前記車両履歴情報格納部に格納されている車両履歴情報を前記認証端末に対して送信することを特徴とする、請求項１６に記載の認証システム。
【請求項２１】　車両に搭載され、当該車両の正当なユ

ーザの認証を行う認証装置と通信可能な入力端末であって、
前記認証装置から送信されてくる、前記車両の使用に伴い変化する車両履歴情報についての質問を出力する端末側出力部と、
前記車両履歴情報についての質問に対するユーザの回答を入力する端末側回答入力部と、
前記ユーザの回答を前記認証装置に対して送信する端末側通信部とを備える、入力端末。
【請求項２２】　車両の使用に伴い変化する車両履歴情報を検出する車両側装置と通信可能な認証端末であって、
前記車両側装置により検出される車両履歴情報を、当該車両側装置から受信する端末側通信部と、
前記通信部により受信された車両履歴情報を格納する端末側車両履歴情報格納部と、
前記車両履歴情報についての質問を出力する端末側出力部と、
前記車両履歴情報についての質問に対するユーザの回答が入力される端末側回答入力部と、
前記車両履歴情報格納部に格納されている車両履歴情報と前記ユーザの回答とに基づき、正当なユーザであることを認証する端末側ユーザ認証部とを備える、認証端末。
【請求項２３】　車両の正当なユーザの認証を行うための認証方法であって、
前記車両の使用に伴い変化する車両履歴情報を検出するステップと、
前記車両履歴情報を格納するステップと、
前記車両履歴情報についての質問を行うステップと、
前記質問に対するユーザの回答を入力するステップと、
前記車両履歴情報と前記ユーザの回答とに基づき、正当なユーザであることを認証するステップとを備えることを特徴とする、認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、認証装置に関し、より特定的には、車両の正当なユーザの認証を行う認証装置に関する。
【０００２】
【従来の技術】従来から、車両の正当なユーザの認証方法としては、機械的なシリンダキーを利用してエンジンを始動する方法がある。これは、正規のキーなしではエンジン始動を不可能とすることにより、車両の盗難を防止するものである。しかし、機械的なキーは比較的容易に複製が可能であるため、必ずしも十分な盗難防止効果が得られていない。
【０００３】さらに、特公平４－１５１４１号公報にあるように、キーに特定の電子情報を含ませることによりキーの複製を困難にし、車両の盗難防止効果を強化するものがある。しかし、正規のキーが盗難された場合には、車両の盗難を防止することができず、この場合にも盗難防止効果が十分であるとはいえない。
【０００４】そこで、個人認証によって正規のユーザであるかどうかを判定することにより、車両の盗難を防止する方法が考えられる。この方法として、例えば、特開平７－１６８９３０号公報、特開２０００－１６８５０２号公報、特開２０００－８５５３６号公報にあるように、指紋や目の虹彩といった生体的特徴を検出することで個人照合を行い、正規なユーザであることの認証を行う車両用ユーザ認識装置が提案されている。また、個人認証により正規のユーザであることを認証する他の方法として、認証のキーとしてパスワードを用いる認証装置が従来から知られている。
【０００５】
【発明が解決しようとする課題】生体的特徴を検出することにより正規のユーザであることを認証する方法では、生体的特徴を検出するユニットを必要とするため、認証装置が大型化、高コスト化してしまう。一方、パスワードを用いた方法では、同じパスワードを使用し続けると、パスワードを盗用される可能性が高くなり、認証の安全性が低くなる。そのため、定期的にパスワードを変更する必要があるので、ユーザの負担が大きくなる。
【０００６】それ故に、本発明の目的は、今までにない認証の方法により、小型化および低コスト化が可能で、かつ、安全性の高い、車両を操作した正当なユーザを認証する認証装置および認証方法を提供することである。
【０００７】
【課題を解決するための手段および発明の効果】本発明は、上記のような目的を達成するために、以下に述べるような特徴を有している。
【０００８】第１の発明は、車両の正当なユーザの認証を行うための認証装置であって、車両の使用に伴い変化する車両履歴情報を検出する車両履歴情報検出部と、車両履歴情報検出部により検出された車両履歴情報を格納する車両履歴情報格納部と、車両履歴情報についての質問を出力する出力部と、車両履歴情報についての質問に対するユーザの回答を入力する回答入力部と、車両履歴情報格納部に格納されている車両履歴情報とユーザの回答とに基づき、正当なユーザであることを認証するユーザ認証部とを備えている。
【０００９】上記第１の発明によれば、車両履歴情報をユーザ認証に用いることができる。車両履歴情報とは、車両の移動や時間の経過等により、車両の使用に伴って変化し、車両を識別することができる情報をいう。例えば、通過した地点の履歴、出発地若しくは目的地のような地点に関する情報、移動した経路の履歴のような経路に関する情報、ガソリン残量、車両の速度に関する情報、および、ＶＩＣＳ（Ｖｅｈｉｃｌｅ　Ｉｎｆｏｒｍａｔｉｏｎ　ａｎｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｓ

ｙｓｔｅｍ）受信履歴に関する情報は、車両履歴情報に含まれる。このような車両履歴情報は、車両を操作した正当なユーザのみが記憶している情報であり、しかも車両に乗車するたびに絶えず変化する情報である。従って、車両履歴情報を認証に用いることにより、固定のパスワードを認証情報として用いる場合に比べて、他人に盗用される可能性が少なくなるので、認証の安全性が高くなる。また、生体的特徴を用いて認証を行う認証装置と比べると、生体的特徴を検出する検出ユニットを必要とすることなく認証を行うことができるので、小型化および低コスト化が可能である。

【００１０】第２の発明は、第１の発明に従属する発明であって、車両履歴情報は、１以上の所定地点についての履歴情報を表す地点履歴情報を含んでいる。

【００１１】上記第２の発明によれば、地点履歴情報をユーザ認証に用いることができる。地点履歴情報とは、その地点について、車両が以前に通過したり、立ち寄ったりした履歴を表す情報である。このような地点履歴情報は、ユーザが特に意識しなくとも比較的容易に記憶しておくことができる情報である。従って、上記第２の発明によれば、地点履歴情報を認証に用いることにより、ユーザの記憶のための負担を少なくすることができる。

【００１２】第３の発明は、第２の発明に従属する発明であって、地点履歴情報は、ユーザにより予め登録された１以上の地点を前回通過した日時と、車両に前回乗車した日時とについての情報とを含んでいる。

【００１３】上記第３の発明によれば、ユーザがよく通過する地点またはよく利用する施設を選択して、選択した地点に関する履歴を認証に用いることができる。従って、ユーザは、認証を行う際の質問に対する回答を容易に記憶しておくことができるので、ユーザの記憶のための負担が軽減される。また、上記第３の発明によれば、前回通過した日および時刻という、ユーザが容易に記憶しておくことができる情報について質問が行われる。これによっても、ユーザの記憶のための負担が軽減される。

【００１４】第４の発明は、第３の発明に従属する発明であって、ユーザ認証部は、登録地点から任意の地点を選出し、出力部は、ユーザ認証部により選出された地点について、車両に前回乗車したときに通過したかどうかの質問と、車両に前回乗車したときに通過した場合は、車両に前回乗車したときに通過した時刻の質問とを出力する。

【００１５】上記第４の発明によれば、ユーザ認証部が自動的に選出した地点について、地点の履歴についての質問を行うことができる。従って、地点を選択する操作を行う必要がないため、ユーザの操作の負担が軽減される。

【００１６】第５の発明は、第３の発明に従属する発明であって、回答入力部は、登録地点のうちユーザにより選択された地点を入力し、出力部は、回答入力部により入力された地点について、車両に前回乗車したときに通過した時刻の質問を出力する。

【００１７】上記第５の発明によれば、ユーザが自ら選択した地点について、前回通過した時刻の質問を行うことができる。従って、ユーザは、自分が履歴を記憶している地点について通過時刻を回答すればよいので、ユーザの記憶のための負担がさらに軽減される。

【００１８】第６の発明は、第１の発明に従属する発明であって、ユーザに関する固有の情報および／またはユーザにより予め設定されるパスワードを含む個人情報を格納する個人情報格納部をさらに備え、出力部は、車両に前回乗車してからの経過期間が所定期間以内である場合は、車両履歴情報についての質問を出力し、経過期間が所定期間を越える場合は、個人情報についての質問を出力し、回答入力部は、経過期間が所定期間以内である場合は、車両履歴情報についての質問に対するユーザの回答を入力し、経過期間が所定期間を越える場合は、個人情報についての質問に対するユーザの回答を入力し、ユーザ認証部は、経過期間が所定期間以内である場合は、車両履歴情報とユーザの回答とに基づき、正当なユーザであるかどうかを判定し、経過期間が所定期間を越える場合は、個人情報とユーザの回答とに基づき、正当なユーザであることを認証する。

【００１９】上記第６の発明によれば、ユーザが所定期間車両に乗車しなかった場合、個人情報を用いた認証が行われる。ユーザは、一般的に、前回乗車してからある程度期間が経過すると、車両履歴情報を忘れてしまう。このような場合には、ユーザが確実に記憶しておくことができる個人情報を認証に用いる方が、ユーザの記憶のための負担が小さくなる。以上より、上記第６の発明により、長期間車両に乗車しなかった場合にも、ユーザの記憶のための負担を軽減しつつ、確実に認証を行う認証装置を提供することができる。

【００２０】第７の発明は、第１の発明に従属する発明であって、車両のエンジンへの給電を行う電力制御部をさらに備え、ユーザ認証部は、正当なユーザであることを認証した場合、電力制御部に給電を開始させる。

【００２１】上記第７の発明によれば、正当なユーザであることが認証された場合のみ、車両の使用が可能となる。従って、車両履歴情報を用いた認証装置により車両の盗難を防止することができる。

【００２２】第８の発明は、第１の発明に従属する発明であって、車両のエンジンへの給電を行う電力制御部と、キーを用いた認証を行い、正規のキーであることを認証した場合、電力制御部に給電を開始させるキー認証部と、車両の使用制限命令を入力する制限命令入力部とをさらに備え、ユーザ認証部は、車両使用の制限命令に応じて認証を行い、正当なユーザであると認証した場合、キー認証部によって電力制御部が給電を開始するこ

とを禁止する。

【００２３】上記第８の発明によれば、認証装置は、車両履歴情報を用いた認証によって、キーを用いた認証による車両の使用を禁止することができる。従って、キーが盗難された場合であっても、ユーザは、車両履歴情報を用いた認証を行うことにより、車両の盗難を防止することができる。さらに、通常の車両使用時は、ユーザはキーを用いた認証のみを行えばよいので、車両使用時における認証の手間が少なくなる。

【００２４】第９の発明は、第８の発明に従属する発明であって、車両の使用命令を入力する使用命令入力部をさらに備え、ユーザ認証部は、車両の使用命令に応じて認証を行い、正当なユーザであると認証した場合、電力制御部に給電を開始させる。

【００２５】上記第９の発明によれば、認証装置は、車両履歴情報を用いた認証により、車両の使用を可能とすることができる。従って、ユーザは、キーを用いた認証による車両の使用が制限されている場合であっても、車両を使用することができる。

【００２６】第１０の発明は、第１の発明に従属する発明であって、車両のエンジンへの給電を行う電力制御部と、キーを用いた認証を行い、正規のキーであることを認証した場合、電力制御部に対して給電を開始させるキー認証部と、電力制御部による給電が開始されてから所定時間内に、認証部が正当なユーザであることを認証しなかった場合、車両が不正に使用されていることをユーザに通報する通報部とをさらに備えている。

【００２７】上記第１０の発明によれば、キーを用いた認証のみが車両の乗車時に行われ、車両履歴情報を用いた認証は、車両の使用開始後に行われる。従って、ユーザは、車両の乗車時には、簡単で短時間で行うことのできる認証のみを行えばよい。また、車両履歴情報を用いた認証が行われなかった場合、正当なユーザに対する通報が行われる。従って、正当なユーザが車両を使用する場合であれば、車両履歴情報を用いた認証を行わなくとも、問題はない。以上より、上記第１０の発明によれば、正当なユーザは、キーを用いた簡単な認証により車両を使用することができる。さらに、上記第１０の発明によれば、不正に使用するユーザに対しては、車両履歴情報を用いた安全性の高い認証を行うことができる。

【００２８】第１１の発明は、第１の発明に従属する発明であって、カーナビゲーションシステムの一部として構成されたことを特徴とする。

【００２９】上記第１１の発明によれば、認証装置は、カーナビゲーションシステムを用いて構成される。カーナビゲーションシステムは、ユーザからの情報を入力する機能、ユーザに対し画像、音声等により情報を出力する機能、車両履歴情報を記憶する機能および、車両の現在位置を検出する機能を有している。従って、本発明の認証装置を実現するために、カーナビゲーションシステムを利用することが可能である。以上より、上記第１１の発明によれば、新たな装置を設置する必要なく、本発明の認証装置を実現することができる。

【００３０】第１２の発明は、車両の使用に伴い変化する車両履歴情報についての質問の出力および質問に対するユーザの回答の入力を行う入力端末と通信可能な認証装置であって、車両履歴情報を検出する車両履歴情報検出部と、車両履歴情報検出部により検出された車両履歴情報を格納する車両履歴情報格納部と、車両履歴情報についての質問を入力端末に送信し、質問に対するユーザの回答を入力端末から受信する通信部と、車両履歴情報格納部に格納されている車両履歴情報とユーザの回答とに基づき、正当なユーザであることを認証するユーザ認証部とを備えている。

【００３１】上記第１２の発明によれば、固定のパスワードを認証情報として用いる場合に比べて、他人に盗用される可能性が少なくなるので、認証の安全性が高くなる。また、生体的特徴を用いて認証を行う認証装置と比べると、生体的特徴を検出する検出ユニットを必要とすることなく認証を行うことができるので、小型化および低コスト化が可能である。

【００３２】さらに、上記第１２の発明によれば、ユーザは、入力端末を用いて車両の外から認証を行うことができる。従って、ユーザは、車両の乗車前に車両履歴情報を用いた認証を予め行っておくことができる。これにより、車両に乗車した際に面倒な認証を行う必要がなくなり、乗車時におけるユーザの手間を省くことができる。

【００３３】第１３の発明は、車両に搭載され、車両の正当なユーザの認証を行う認証装置と、認証装置と通信可能な入力端末とを含む認証システムであって、認証装置は、車両の使用に伴い変化する車両履歴情報を検出する車両履歴情報検出部と、車両履歴情報検出部により検出された車両履歴情報を格納する車両履歴情報格納部と、車両履歴情報についての質問を入力端末に対して送信し、質問に対するユーザの回答を入力端末から受信する通信部と、車両履歴情報格納部に格納されている車両履歴情報とユーザの回答とに基づき、正当なユーザであることを認証するユーザ認証部とを備え、入力端末は、認証装置から送信されてくる車両履歴情報についての質問を出力する端末側出力部と、車両履歴情報についての質問に対するユーザの回答を入力する端末側回答入力部と、ユーザの回答を認証装置に対して送信する端末側通信部とを備えている。

【００３４】上記第１３の発明によれば、固定のパスワードを認証情報として用いる場合に比べて、他人に盗用される可能性が少なくなるので、認証の安全性が高くなる。また、生体的特徴を用いて認証を行う認証装置と比べると、生体的特徴を検出する検出ユニットを必要とすることなく認証を行うことができるので、小型化および

低コスト化が可能である。

【００３５】さらに、上記第１３の発明によれば、ユーザは、入力端末を用いて車両の外から認証を行うことができる。従って、ユーザは、車両の乗車前に車両履歴情報を用いた認証を予め行っておくことができる。これにより、車両の乗車した際に面倒な認証を行う必要がなくなり、乗車時におけるユーザの手間を省くことができる。

【００３６】第１４の発明は、第１３の発明に従属する発明であって、認証装置は、車両のエンジンへの給電を行う電力制御部と、キーを用いた認証を行い、正規のキーであることを認証した場合、電力制御部に対して給電を開始させるキー認証部とをさらに備え、入力端末は、車両の使用制限命令を入力する端末側制限命令入力部をさらに備え、ユーザ認証部は、車両の使用制限命令に応じて認証を行い、正当なユーザであると認証した場合、キー認証部によって電力制御部が給電を開始することを禁止する。

【００３７】上記第１４の発明によれば、認証システムは、車両履歴情報を用いた認証によって、キーを用いた認証による車両の使用を禁止することができる。従って、キーが盗難された場合であっても、ユーザは、車両履歴情報を用いた認証を行うことにより、車両の盗難を防止することができる。また、通常の車両使用時は、ユーザはキーを用いた認証のみを行えばよいので、車両使用時における認証の手間が少なくなる。

【００３８】さらに、上記第１４の発明によれば、入力端末を用いることによって車両の使用を禁止することができる。すなわち、ユーザは、車両の中に入らなくとも、車両の外から車両の使用を禁止することができる。従って、キーが盗難された場合に、ユーザは、スペアキーを持っていないため車内に入ることができない場合でも、車両の使用を禁止することができる。

【００３９】第１５の発明は、第１４の発明に従属する発明であって、入力端末は、車両の使用命令を入力する端末側使用命令入力部をさらに備え、ユーザ認証部は、車両の使用命令に応じて認証を行い、正当なユーザであると認証した場合、電力制御部に給電を開始させる。

【００４０】上記第１５の発明によれば、認証システムは、車両履歴情報を用いた認証により、車両の使用を可能とすることができる。従って、ユーザは、キーを用いた認証による車両の使用が制限されている場合であっても、車両を使用することができる。

【００４１】第１６の発明は、車両に搭載される車両側装置と、車両側装置と通信可能な認証端末とを含む認証システムであって、車両側装置は、車両の使用に伴い変化する車両履歴情報を検出する車両履歴情報検出部と、車両履歴情報検出部により検出された車両履歴情報を認証端末に対して送信する通信部とを備え、認証端末は、通信部から送信されてくる車両履歴情報を格納する端末側車両履歴情報格納部と、車両履歴情報についての質問を出力する端末側出力部と、車両履歴情報についての質問に対するユーザの回答を入力する端末側回答入力部と、端末側車両履歴情報格納部に格納されている車両履歴情報とユーザの回答とに基づき、正当なユーザであることを認証する端末側ユーザ認証部とを備えている。

【００４２】上記第１６の発明によれば、車両の使用に伴い変化する車両履歴情報が認証に用いられる。従って、固定のパスワードを認証情報として用いる場合に比べて、他人に盗用される可能性が少なくなるので、認証の安全性が高くなる。また、生体的特徴を用いて認証を行う認証装置と比べると、生体的特徴を検出する検出ユニットを必要とすることなく認証を行うことができるので、装置の小型化および低コスト化が可能である。

【００４３】さらに、上記第１６の発明によれば、ユーザは、認証端末を用いて車両の外で認証を行うことができる。従って、ユーザは、車両の乗車前に車両履歴情報を用いた認証を予め行っておくことができる。これにより、車両の乗車した際に面倒な認証を行う必要がなくなり、乗車時におけるユーザの手間を省くことができる。

【００４４】第１７の発明は、第１６の発明に従属する発明であって、認証端末は、端末側ユーザ認証部による認証結果を、車両側装置に対して送信する端末側通信部をさらに備え、車両側装置は、端末側通信部から受信した認証結果に基づいて、車両の盗難を防止するための処理を行う盗難防止処理部をさらに備えている。

【００４５】上記第１７の発明によれば、車両側装置は、車両履歴情報を用いた認証の結果を、車両の盗難防止に用いることができる。従って、車両側装置は、安全性の高い認証を用いることにより、車両の盗難防止効果を高めることができる。

【００４６】第１８の発明は、第１７の発明に従属する発明であって、盗難防止処理部は、車両のエンジンへの給電を行う電力制御部を含み、車両側装置は、キーを用いた認証を行い、正規のキーであることを認証した場合、電力制御部に対して給電を開始させるキー認証部をさらに備え、認証端末は、車両の使用制限命令を入力する端末側制限命令入力部をさらに備え、端末側ユーザ認証部は、車両の使用制限命令に応じて認証を行い、正当なユーザであると認証した場合、端末側通信部に電力制御部に対して給電禁止信号を送信させ、それによって、キー認証部によって電力制御部が給電を開始することを禁止する。

【００４７】上記第１８の発明によれば、認証システムは、車両履歴情報を用いた認証により、キーを用いた認証による車両の使用を禁止することができる。従って、キーが盗難された場合であっても、ユーザは、車両履歴情報を用いた認証を行うことにより、車両の盗難を防止することができる。また、通常の車両使用時は、ユーザはキーを用いた認証のみを行えばよいので、車両使用時

における認証の手間が少なくなる。

【００４８】さらに、上記第１８の発明によれば、入力端末を用いることによって車両の使用を禁止することができる。すなわち、ユーザは、車両の中に入らなくとも、車両の外から車両の使用を禁止することができる。従って、キーが盗難された場合に、ユーザは、スペアキーを持っていないため車内に入ることができない場合でも、車両の使用を禁止することができる。

【００４９】第１９の発明は、第１８の発明に従属する発明であって、認証端末は、車両の使用命令を入力する端末側使用命令入力部をさらに備え、端末側ユーザ認証部は、車両の使用命令に応じて認証を行い、正当なユーザであると認証した場合、端末側通信部に電力制御部に対して給電信号を送信させ、それによって、電力制御部に給電を開始させる。

【００５０】上記第１９の発明によれば、認証システムは、車両履歴情報を用いた認証により、車両の使用を可能とすることができる。従って、ユーザは、キーを用いた認証による車両の使用が制限されている場合であっても、車両を使用することができる。

【００５１】第２０の発明は、第１６の発明に従属する発明であって、車両側装置は、車両履歴情報検出部により検出された車両履歴情報を格納する車両履歴情報格納部をさらに備え、通信部は、車両の使用が終了したとき、車両履歴情報格納部に格納されている車両履歴情報を認証端末に対して送信する。

【００５２】上記第２０の発明によれば、前回までの車両の履歴情報が認証端末に格納されることとなる。従って、常に最新の車両履歴情報が認証端末に格納されるので、認証システムは、正確な認証を行うことができる。

【００５３】第２１の発明は、車両に搭載され、車両の正当なユーザの認証を行う認証装置と通信可能な入力端末であって、認証装置から送信されてくる、車両の使用に伴い変化する車両履歴情報についての質問を出力する端末側出力部と、車両履歴情報についての質問に対するユーザの回答を入力する端末側回答入力部と、ユーザの回答を認証装置に対して送信する端末側通信部とを備えている。

【００５４】上記第２１の発明によれば、入力端末は、認証装置を用いることにより車両履歴情報によって認証を行うことができる。すなわち、ユーザは、車両の外にいる場合であっても、予め認証を行っておくことができる。これにより、車両の乗車した際に面倒な認証を行う必要がなくなり、乗車時におけるユーザの手間を省くことができる。

【００５５】第２２の発明は、車両の使用に伴い変化する車両履歴情報を検出する車両側装置と通信可能な認証端末であって、車両側装置により検出される車両履歴情報を、車両側装置から受信する端末側通信部と、通信部により受信された車両履歴情報を格納する端末側車両履歴情報格納部と、車両履歴情報についての質問を出力する端末側出力部と、車両履歴情報についての質問に対するユーザの回答が入力される端末側回答入力部と、車両履歴情報格納部に格納されている車両履歴情報とユーザの回答とに基づき、正当なユーザであることを認証する端末側ユーザ認証部とを備えている。

【００５６】上記第２２の発明によれば、通信端末は、車両履歴情報を用いた認証を行う。従って、固定のパスワードを認証情報として用いる場合に比べて、他人に盗用される可能性が少なくなり、認証の安全性が高くなる。また、生体的特徴を用いて認証を行う認証装置と比べると、生体的特徴を検出する検出ユニットを必要とすることなく認証が行えるので、小型化および低コスト化が可能である。

【００５７】さらに、上記第２２の発明によれば、ユーザは、認証端末を用いて車両の外で認証を行うことができる。従って、ユーザは、車両の乗車前に車両履歴情報を用いた認証を予め行っておくことができる。これにより、車両の乗車した際に面倒な認証を行う必要がなくなり、乗車時におけるユーザの手間を省くことができる。

【００５８】第２３の発明は、車両の正当なユーザの認証を行うための認証方法であって、車両の使用に伴い変化する車両履歴情報を検出するステップと、車両履歴情報を格納するステップと、車両履歴情報についての質問を行うステップと、質問に対するユーザの回答を入力するステップと、車両履歴情報とユーザの回答とに基づき、正当なユーザであるかどうかを判定するステップとを備えている。

【００５９】上記第２３の発明によれば、車両の使用に伴い変化する車両履歴情報が認証に用いられる。従って、固定のパスワードを認証情報として用いる場合に比べて、他人に盗用される可能性が少なくなるので、認証の安全性が高くなる。また、生体的特徴を用いて認証を行う認証装置と比べると、生体的特徴を検出する検出ユニットを必要とすることなく認証が行えるので、小型化および低コスト化が可能である。

【００６０】

【発明の実施の形態】最初に、本実施形態に係る認証装置の概要について説明する。本発明において認証に用いる車両履歴情報は、車両の使用に伴い変化するものである。従って、車両履歴情報を用いて認証を行えば、盗用される可能性が少なく、定期的に変更する必要がないため、安全性の高い認証を行うことができる。また、このような車両履歴情報は、ユーザが特に意識しなくとも記憶しておくことができる情報が望ましい。そのような情報を用いれば、ユーザは無理に記憶する必要がなく、ユーザの記憶のための負担が少なくなるからである。そこで、本実施形態に係る認証装置は、所定の地点についての履歴情報を用いて認証を行う。ここで、所定の地点とは、ユーザが予め登録することができる任意の地点であ

り、ユーザが日頃よく通過する地点を複数登録しておくことが望ましい。具体的には、本実施形態に係る認証装置は、前回乗車したときには所定の地点を通過したか、および、通過した場合は何日の何時頃に通過したか、という質問をユーザに回答させることにより、認証を行う。なお、本実施形態の説明において、ユーザが登録した所定の地点を登録地点と呼ぶ。

【００６１】また、本実施形態に係る認証装置は、所定地点についての履歴情報と個人情報とを併用して認証を行う。ここで、個人情報とは、ユーザに固有の情報をいう。典型的には、個人情報として、ユーザの生年月日、家族構成、または、ユーザが予め設定したパスワードが用いられる。本実施形態に係る認証装置は、所定地点についての履歴情報とユーザが予め設定したパスワードとを併用して認証を行う。

【００６２】以下、図１～図９を用いて、第１の実施形態を詳しく説明する。図１は、第１の実施形態に係る認証装置を搭載した車両の構成を示すブロック図である。認証装置は、車両において一般に使用されているカーナビゲーションシステムを利用した形態である。図１において、カーナビゲーションシステム１は、入力部１１と、出力部１２と、記憶部１３と、情報処理部１４と、現在位置検出部１５とを備える。また、車両は、キーシリンダ２１１およびシリンダキー２１２と、電源２２と、エンジン２３と、電力制御部２４とを備える。

【００６３】入力部１１は、経路探索の際に目的地および認証の際に質問に対する回答を入力する。出力部１２は、経路案内のための地図データおよび認証を行う際の質問を、画像および音声により出力する。具体的には、出力部１２は、経路案内のための地図データおよび認証を行う際の質問を画像により表示する表示部１２１と、認証を行う際の質問を音声により出力する音声出力部１２２とを備える。記憶部１３は、経路探索や経路案内に必要な地図データに加えて、認証に必要となる車両履歴情報および個人情報を格納する。記憶部１３の詳細は、図２において示されている。

【００６４】情報処理部１４は、典型的にはＣＰＵによって構成され、従来のカーナビゲーションシステムが有するナビゲーション機能の他、正当なユーザであることを認証する機能および地点についての履歴情報を更新する機能を有する。情報処理部１４の詳細は、図４において示されている。現在位置検出部１５は、車両の現在位置を算出するために必要なデータを検出する。現在位置検出部１５は、ＧＰＳ受信機１５１と、速度センサ１５２と、方位センサ１５３とを備える。キーシリンダ２１１およびシリンダキー２１２は、電源２２からカーナビゲーションシステム１に電力を供給するスイッチとして用いられる。電源２２は、カーナビゲーションシステム１および車両のエンジン２３に電力を供給する。電源２２からエンジン２３への給電は、電力制御部２４により制御されている。すなわち、電力制御部２４は、カーナビゲーションシステム１からの給電許可信号に応答して、電源２２からエンジン２３への給電を開始する。

【００６５】図2は、図１に示す記憶部１３の詳細な構成を示すブロック図である。記憶部１３は、地図データ格納部１３１と、車両履歴情報格納部１３２と、個人情報格納部１３３とを備える。地図データ格納部１３１は、現在位置の特定を行うためのロケーションに必要な地図データを格納する。車両履歴情報格納部１３２は、認証に必要となる車両履歴情報を格納する。本実施形態において、車両履歴情報格納部１３２は、地点についての履歴情報を表す地点情報データテーブル１３２１および前回乗車した日時を表す前回乗車日時データ１３２２を格納する。地点情報データテーブル１３２１については、図３において詳細に示されている。個人情報格納部１３３は、ユーザが予め設定するパスワードを表すパスワードデータ１３３１を格納する。

【００６６】図3は、図２に示す地点情報データテーブル１３２１の一例を示す図である。一般的に、従来のカーナビゲーションシステムは、目的地の設定を容易にする目的で、任意の地点の位置情報を登録することが可能である。このような従来のカーナビゲーションシステムは、登録された地点の名称および位置のデータを格納したデータテーブルを保持している。ここで、本実施形態に係る認証装置における地点情報データテーブル１３２１は、従来のカーナビゲーションシステムが保持するデータテーブルを拡張したものである。すなわち、地点情報データテーブル１３２１は、登録地点ごとにそれぞれ、登録地点の名称を表す地点名データと、登録地点の位置を表す位置データとに加えて、前回登録地点を通過した日付を表す通過日データと、前回登録地点を通過した時刻を表す通過時刻データとを格納している。地点名データは、ユーザが地点を登録する際に、ユーザの覚えやすい名称を登録できるようにしておくことが望ましい。位置データは、登録地点の通過日データおよび通過時刻データを更新する際に参照される。通過日データおよび通過時刻データは、認証を行う際に用いられる。

【００６７】図4は、情報処理部１４の詳細な構成を示すブロック図である。一般的に、従来のカーナビゲーションシステムは、ＧＰＳ受信機、速度センサ、方位センサからの情報に基づき、車両の現在位置を算出し、算出された現在位置と目的地との経路探索および経路案内を行うことが可能である。このような従来のカーナビゲーションシステムは、車両の現在位置を算出するロケーション機能と、経路探索を行う経路探索機能と、経路案内を行う経路案内機能とを備えている。ここで、本実施形態に係る認証装置における情報処理部１４は、従来のカーナビゲーションシステムの機能を拡張したものであって、ロケーション部１４１と、経路探索部１４２と、経路案内部１４３とに加えて、認証部１４４と、車両履歴

情報更新部１４５とを備える。ロケーション部１４１は、現在位置検出部１５が検出する情報に基づき、車両の現在位置を算出する。経路探索部１４２は、ロケーション部１４１により算出される車両の現在位置のデータ、記憶部１３に記憶されている地図データおよび入力部１１から出力される目的地のデータに基づき、任意の目的地までの経路を探索する。経路案内部１４３は、経路探索部１４２により探索された経路の情報および記憶部１３に記憶されている地図データに基づき、出力部１２に経路を表示させることにより、経路案内を行う。なお、ロケーション部１４１、経路探索部１４２および経路案内部１４３は、上述のように、従来のカーナビゲーションシステムにおいて構成されるものである。

【００６８】認証部１４４は、ユーザが車両に乗車する際に認証処理を行う。具体的には、認証部１４４は、認証を行う際に、質問の選択、地点情報および個人情報の比較、並びに質問に対するユーザの回答が正解かどうかの判定を行う。認証処理の詳細は、図７～図９において示されている。また、認証部１４４は、認証が成功した場合、電力制御部２４に対して、給電許可信号を送信する。車両履歴情報更新部１４５は、車両履歴情報の更新処理を行う。具体的には、車両履歴情報更新部１４５は、地点情報データテーブル１３２１を更新すべきかどうかの判定並びに地点情報データテーブル１３２１の更新を行う。更新処理の詳細は、図６に示されている。

【００６９】図５は、第１の実施形態に係るカーナビゲーションシステム１における、認証に必要な処理の流れを示すフローチャートである。まず、カーナビゲーションシステム１は、認証に用いる車両履歴情報の更新処理を行う（ステップＳ１）。具体的には、車両履歴情報の更新処理は、車両履歴情報更新部１４５により、前回の車両乗車中に行われる。また、情報処理部１４において他の処理が行われている場合、車両履歴情報の更新処理は、ロケーション部１４１が現在位置を特定するごとに割り込み処理の形で、または、サブルーチン呼び出しの形で行われる。なお、サブルーチンステップＳ１の詳細は、図６に示されている。

【００７０】次に、カーナビゲーションシステム１は、認証処理を行う（ステップＳ２）。具体的には、認証処理は、認証部１４４により、ユーザが車両に乗車する際に行われる。すなわち、認証処理は、ユーザがシリンダキー２１２をキーシリンダ２１１に差し込み、カーナビゲーションシステム１に電源２２から電力が供給されることにより開始される。なお、サブルーチンステップＳ２の詳細は、図７～図９に示されている。

【００７１】図６は、図５のサブルーチンステップＳ１の詳細な処理を示すフローチャートである。ここで、車両履歴情報更新部１４５は、地点情報データテーブル１３２１の位置データとして、カーナビゲーションシステム１において用いられる緯度、経度の座標データを用いて更新処理を行う。以下、図６を参照して車両履歴情報の更新処理について説明する。

【００７２】まず、車両履歴情報更新部１４５は、ロケーション部１４１により算出された車両の現在位置を表す位置データを読み込む（ステップＳ１１）。ステップＳ１１の処理は、ロケーション部１４１が現在位置を特定したときに行われる。次に、車両履歴情報更新部１４５は、車両の現在位置と各登録地点の位置が一致するかを各登録地点ごとに判定する（ステップＳ１２）。ステップＳ１２における判定は、ロケーション部１４１により算出された車両の現在位置を表す位置データと、地点情報データテーブル１３２１の各登録地点についての位置データとを比較することにより行われる。

【００７３】ステップＳ１２における判定処理をより詳細に説明すると、まず、車両履歴情報更新部１４５は、車両の現在位置を表す座標データと登録地点の位置を表す座標データとから、車両の現在位置と登録地点の位置との距離を算出する。算出された距離が所定値以下である場合、車両履歴情報更新部１４５は、車両の現在位置と登録地点の位置とが一致すると判定する。一方、算出された距離が所定値を越えている場合、車両履歴情報更新部１４５は、車両の現在位置と登録地点の位置とが一致しないと判定する。ここで、所定値は、車両が登録地点の前の道路を通過すれば、車両の現在位置と登録地点の位置とが一致すると判定される程度の距離（例えば、２０ｍ）に設定される。

【００７４】ステップＳ１２の判定処理において、車両の現在位置と登録地点の位置とが一致する場合、車両履歴情報更新部１４５は、地点情報データテーブル１３２１の内容を更新する（ステップＳ１３）。ステップＳ１３における更新は、一致すると判定された登録地点の地点情報データテーブル１３２１の通過日データおよび通過時刻データを、それぞれ、現在の日付および時刻を表すデータに書き換えることにより行われる。一方、車両の現在位置と登録地点の位置とが一致しない場合、車両履歴情報更新部１４５は、地点情報データテーブル１３２１の内容を更新せずに、ステップＳ１４の処理を行う。

【００７５】次に車両履歴情報更新部１４５は、車両が使用中であるか否か判定する。車両が使用中である場合、車両履歴情報更新部１４５は、ステップＳ１１～ステップＳ１３の処理を繰り返す。一方、車両が使用中でない場合、車両履歴情報更新部１４５は、更新処理を終了する。

【００７６】図７は、図５のサブルーチンステップＳ２の詳細な動作を示すフローチャートである。まず、認証部１４４は、前回乗車してからの経過期間が、所定期間以内であるかどうかを判定する（ステップＳ２１）。前回乗車してからの経過期間は、車両履歴情報格納部１３２に格納されている前回乗車日時データ１３２２と、現

在の日時を表すデータとから算出される。前回乗車してからの経過期間が所定期間以内である場合、認証部１４４は、登録地点についての履歴情報に関する質問により認証を行う（ステップＳ２２）。このサブルーチンステップＳ２２の詳細は、図8に示されている。ここで、所定期間は、ユーザが前回乗車したときの通過履歴を覚えておくことができる適当な期間（例えば、3日）に設定される。また、所定期間は、ユーザが予め設定できるようにしておくことが望ましい。一方、前回乗車してからの経過期間が所定期間を越える場合、認証部１４４は、個人情報に関する質問により認証を行う（ステップＳ２３）。このサブルーチンステップＳ２３の詳細は、図9に示されている。

【００７７】図8は、図7のサブルーチンステップＳ２２の詳細な動作を示すフローチャートである。認証部１４４は、複数の登録地点の中から、任意の一の地点を選出する（ステップＳ２２０１）。ステップＳ２２０１における選出は、乱数等を用いてランダムに行われることが望ましい。地点が選出された後、認証部１４４は、選出された登録地点について、前回乗車したときにその登録地点を通過したかどうかを、出力部１２を用いて質問を行う（ステップＳ２２０２）。入力部１１は、質問に対するユーザの回答を入力し、認証部１４４に出力する。ここでの回答形式は、ＹｅｓまたはＮｏの二者択一形式である。次に、認証部１４４は、質問に対する回答が正解であるかどうかを判定する（ステップＳ２２０３）。ステップＳ２２０３における判定は、地点情報データテーブル１３２１の中の選出された登録地点についての通過日データおよび通過時刻データと、前回乗車日時データ１３２２と、入力部１１から出力されるデータとを比較することにより行われる。

【００７８】ステップＳ２２０３における判定処理をより詳細に説明すると、選出された登録地点についての通過日時が前回乗車日時より後である場合に、ユーザの回答がＹｅｓである場合（すなわち、通過したと回答した場合）、認証部１４４は、質問に対する回答は正解であると判定する。また、同様に、選出された登録地点についての通過日時が前回乗車日時よりも前である場合に、ユーザの回答がＮｏである場合（すなわち、通過していないと回答した場合）、認証部１４４は、質問に対する回答は正解であると判定する。一方、選出された登録地点についての通過日時が前回乗車日時よりも後である場合に、ユーザの回答がＮｏである場合（すなわち、通過していないと回答した場合）、または、選出された登録地点についての通過日時が前回乗車日時よりも前である場合に、ユーザの回答がＹｅｓである場合（すなわち、通過したと回答した場合）、認証部１４４は、質問に対する回答は不正解であると判定する。

【００７９】質問に対する回答が正解である場合、認証部１４４は、選出された登録地点を前回乗車したときに通過したかどうかを判定する（ステップＳ２２０４）。ステップＳ２２０４における判定は、地点情報データテーブル１３２１の中の選出された登録地点についての通過日データおよび通過時刻データと、前回乗車日時データ１３２２とを比較することにより行われる。選出された登録地点についての通過日時が前回乗車日時より後である場合、認証部１４４は、出力部１２を用いて選出された登録地点の前回通過した時刻について質問を行う（ステップＳ２２０５）。一方、選出された登録地点についての通過日時が前回乗車日時よりも前である場合、認証部１４４は、選出された登録地点についての質問を終了する。選出された登録地点の前回通過した時刻についての質問に対し、ユーザは、入力部１１を用いて、選出された登録地点について前回乗車した際に通過した時刻を入力する。認証部１４４は、質問に対する回答が正解かどうかを判定する（ステップＳ２２０６）。ステップＳ２２０６における判定は、地点情報データテーブル１３２１の中の選出された登録地点についての通過時刻データと、ユーザが入力した時刻を表すデータとを比較することにより行われる。

【００８０】ステップＳ２２０６における判定をより詳細に説明すると、まず、認証部１４４は、選出された登録地点についての通過時刻データと、ユーザが入力した時刻を表すデータとから、通過時刻とユーザが入力した時刻との差を算出する。次に、通過時刻とユーザが入力した時刻との差が所定時間以内である場合、認証部１４４は、質問に対する回答は正解であると判定する。一方、通過時刻とユーザが入力した時刻との差が所定時間を超えている場合、認証部１４４は、質問に対する回答は不正解であると判定する。ここで、所定時間は、大まかな時刻を入力すれば正解と判定されるような時間に設定される。なぜなら、ユーザは、一般に、通過した時刻を正確には記憶していないからである。例えば、所定時間が３０分に設定された場合において、ユーザが入力する時刻が通過時刻から前後３０分の範囲内である場合、認証部１４４は、質問に対する回答は正解であると判定する。

【００８１】ステップＳ２２０６の判定処理において、選出された登録地点についての質問に対する回答が正解である場合、認証部１４４は、ステップＳ２２０１～ステップＳ２２０６の一連の処理で行う質問を所定回数行ったかどうかを判定する（ステップＳ２２０７）。質問を所定回数行った場合、認証部１４４は、認証が成功した場合の処理を行い（ステップＳ２２０８）、処理を終了する。

【００８２】ここで、第1の実施形態においては、認証が成功した場合の処理として、認証部１４４は、電力制御部２４に給電許可信号を送信し、前回乗車日時データ１３２２を更新する。電力制御部２４に給電許可信号が送信されることにより、電源２２の電力がエンジン２３

に供給され、エンジン２３が始動する。また、前回乗車日時データ１３２２の更新は、車両履歴情報格納部１３２に格納されている前回乗車日時データ１３２２を、現在の日時を表すデータに書き換えることにより行われる。これにより、次回車両に乗車したときに、前回乗車日時は正しく記憶されていることになる。

【００８３】一方、ステップＳ２２０７の判定処理において、質問を所定回数行っていない場合、認証部１４４は、所定回数の質問を行うまでステップＳ２２０１～ステップＳ２２０６の一連の処理を繰り返す。ここで、所定回数は、認証の確実性を高める目的で複数の地点について質問を行うために設定されるものであり、ユーザが変更できることが望ましい。

【００８４】次に、登録地点を通過したかどうかの質問に対する回答が不正解である場合の処理について説明する。この場合、認証部１４４は、登録地点を通過したかどうかの質問に対する回答が、Ｙｅｓであったか否かを判定する（ステップＳ２２０９）。登録地点を通過したかどうかの質問に対する回答がＹｅｓである場合、認証部１４４は、出力部１２を用いて選出された登録地点の前回通過した時刻について質問を行う（ステップＳ２２１０）。ステップＳ２２１０の質問は、認証としては意味を持たない。しかし、登録地点を通過したかどうかの質問に対するユーザの回答が正解であった場合と同じ質問を行うことにより、質問に不正解であった不正利用者は、どの質問で不正解となったかを特定することができない。従って、ステップＳ２２１０を設けることにより、不正利用者の不正利用を困難にすることができる。

【００８５】一方、ステップＳ２２０９の判定処理において、登録地点を通過したかどうかの質問に対する回答がＮｏである場合、認証部１４４は、選出された登録地点の前回通過した時刻について質問を行わない。次に、認証部１４４は、認証に失敗した旨を表示部１２１により表示させる（ステップＳ２２１１）。さらに、認証部１４４は、認証に所定回数失敗したかどうかを判定する（ステップＳ２２１２）。認証に所定回数失敗した場合、認証部１４４は、認証が失敗した場合の処理を行い（ステップＳ２２１３）、処理を終了する。なお、第１の実施形態においては、認証が失敗した場合の処理として、認証部１４４は、警告を発する。具体的には、認証部１４４は、出力部１２に警告画像を表示させ、警告音を出力させる。

【００８６】図９は、図７のサブルーチンステップＳ２３の詳細な動作を示すフローチャートである。まず、認証部１４４は、出力部１２を用いてパスワードを要求する（ステップＳ２３０１）。要求に対し、入力部１１は、ユーザからのパスワードを入力し、認証部１４４に出力する。認証部１４４は、入力が正解であるかどうかを判定する（ステップＳ２３０２）。ステップＳ２３０２における判定は、個人情報格納部１３３に格納されているパスワードデータ１３３１と、ユーザが入力したパスワードを表すデータとを比較することにより行われる。入力が正解である場合、認証部１４４は、認証が成功した場合の処理を行い（ステップＳ２３０３）、処理を終了する。なお、第１の実施形態においては、認証が成功した場合の処理として、認証部１４４は、電力制御部２４に給電許可信号を送信し、前回乗車日時データ１３２２を更新する。

【００８７】一方、ステップＳ２３０２の判定処理において、入力が不正解である場合、認証部１４４は、認証に失敗した旨を表示部１２１により表示させる（ステップＳ２３０４）。さらに、認証部１４４は、認証に所定回数失敗したかどうかを判定する（ステップＳ２３０５）。認証に所定回数失敗していない場合、認証部１４４は、ステップＳ２３０１の処理から認証処理の処理をやり直す。一方、認証に所定回数失敗した場合、認証部１４４は、認証が失敗した場合の処理を行い（ステップＳ２３０６）、処理を終了する。なお、第１の実施形態においては、認証が失敗した場合の処理として、認証部１４４は、出力部１２により警告を発する。

【００８８】なお、本実施形態に係る認証装置は、車両履歴情報として所定の地点についての通過履歴を用いて認証を行ったが、車両履歴情報は、これに限らない。例えば、前回乗車したときに移動した地点の履歴または経路の履歴を、車両履歴情報として用いて認証を行ってもよい。また、前回乗車したときの出発地および／または目的地を、車両履歴情報として用いて認証を行ってもよい。さらに、車両履歴情報は、ガソリン残量、前回乗車したときの車両の速度に関する情報、または、ＶＩＣＳ受信履歴等であってもよい。

【００８９】また、本実施形態に係る認証装置は、登録地点の中から認証部１４４がランダムに選出した地点について、前回乗車したときには選出された地点を通過したか、さらに、通過した場合は、何時頃通過したかという質問形式で認証を行った。これに代えて、登録地点の中から任意の地点をユーザ自身が選択し、ユーザにより選択された地点について前回の通過時刻を質問するという質問形式で認証を行ってもよい。この場合、ユーザは、自分が履歴を記憶している地点について通過時刻を回答すればよいので、ユーザの記憶のための負担がさらに軽減される。

【００９０】さらに、本実施形態に係る認証装置は、所定地点の位置を表す位置データとして、緯度および経度の座標データを用いたが、これに代えて、カーナビゲーションシステムにおいて地図データに用いられるリンクおよび／またはノードを、位置データとして用いてもよい。例えば、登録地点から最短距離にある道路に対応するリンクを位置データとして記憶しておく。この方法によれば、車両の現在位置と登録地点の位置が一致するかどうかの判定において、リンクが一致するかどうかを比

較するだけでよいので、判定の処理が簡易になり、処理速度が増すという利点がある。

【００９１】次に、本発明に係る第２の実施形態について説明する。第２の実施形態に係る認証システムは、キーが盗難された場合に、車両の使用を禁止するために認証が行われる形態である。図１０は、第２の実施形態に係る認証システムの構成を示すブロック図である。図１０において、認証システムは、車両に搭載されるカーナビゲーションシステム３と、キーシリンダ２１１およびシリンダキー２１２と、電源２２と、エンジン２３と、電力制御部２４と、ユーザが保持する入力端末４とを備えている。なお、図１０に示す認証システムは、第１の実施形態において用いられる構成要素と同様の構成要素を用いて実現することができる。従って、図１０において、図１と同じ構成要素には同一の参照符号を付し、説明を省略する。

【００９２】カーナビゲーションシステム３は、入力部１１と、出力部１２と、記憶部１３と、情報処理部１４と、現在位置検出部１５と、通信部１６とを備えている。このように、カーナビゲーションシステム３は、第１の実施形態に係るカーナビゲーションシステム１の各構成要素に、通信部１６が加わった構成により実現することができる。通信部１６は、情報処理部１４から入力される情報を、入力端末４に対して送信する。

【００９３】入力端末４は、認証を行う際の質問の出力およびユーザによる回答の入力を行うために用いられる。入力端末４は、入力部４１と、出力部４２と、通信部４３とを備えている。入力部４１は、ユーザの入力により、使用禁止信号を出力する。使用禁止信号とは、車両の使用を禁止するためにカーナビゲーションシステム３に送信される信号である。使用禁止信号を受信することにより、カーナビゲーションシステム３は、車両の使用を禁止するための認証処理を開始する。また、入力部４１は、ユーザにより入力される、認証の際の質問に対する回答を通信部４３に出力する。出力部４２は、認証を行う際の質問を画像により表示し、また、音声により出力する。通信部４３は、カーナビゲーションシステム３の通信部１６との間で無線により通信を行う。

【００９４】次に、車両の使用を禁止する際の、第２の実施形態に係る認証システムの動作を説明する。まず、入力部４１は、ユーザにより車両の使用を禁止する命令が入力されることにより、使用禁止信号を出力する。使用禁止信号は、通信部４３によりカーナビゲーションシステム３に送信される。カーナビゲーションシステム３の通信部１６は、入力端末４からの使用禁止信号を受信し、情報処理部１４に出力する。通信部１６から使用禁止信号が入力されることにより、情報処理部１４の認証部１４４は、認証処理を開始する。すなわち、第２の実施形態においては、認証処理は、認証部１４４が通信部１６から使用禁止信号を受け取ることにより開始される。

【００９５】認証部１４４において行われる認証処理は、図７～図９に示す第１の実施形態における認証処理と同様である。ただし、認証部１４４が行う認証についての質問は、通信部１６を介して入力端末４に送信され、入力端末４の出力部４２により出力される。出力部４２により出力された質問に対して、ユーザは、入力端末４の入力部４１を用いて回答を入力する。入力部４１に入力された回答は、通信部４３を介してカーナビゲーションシステム３に送信される。

【００９６】また、認証部１４４は、図８に示すステップＳ２２０８および図９に示すステップＳ２３０３における、認証が成功した場合の処理として、電力制御部２４に対して給電禁止信号を送信する。給電禁止信号により、電力制御部２４は、シリンダキー２１２がキーシリンダ２１１に差し込まれることによる給電を禁止する。すなわち、認証部１４４から給電禁止信号が送信された後は、シリンダキー２１２がキーシリンダ２１１に差し込まれても、エンジン２３への給電が行われない。

【００９７】また、認証部１４４は、図８に示すステップＳ２２１３および図９に示すステップＳ２３０６における、認証が失敗した場合の処理として、警告を発する。具体的には、認証部１４４は、通信部１６を用いて入力端末４に認証が失敗した旨を通知する。通信部４３を介して通知を受けた出力部４２は、警告画像を表示し、警告音を出力する。

【００９８】以上の動作により、第２の実施形態に係る認証システムは、シリンダキー２１２による車両の使用を禁止する。なお、車両の使用の禁止を解除する場合、上記と同様の認証が行われる。まず、入力部４１は、ユーザにより車両の使用の禁止を解除する命令が入力されることにより、禁止解除信号を出力する。禁止解除信号は、カーナビゲーションシステム３に送信され、認証部１４４に入力される。これにより、情報処理部１４の認証部１４４は、認証処理を開始する。認証が成功したときは、認証部１４４は、電力制御部２４に対して解除信号を送信する。解除信号により、電力制御部２４は、シリンダキー２１２がキーシリンダ２１１に差し込まれることによる給電の禁止を解除する。すなわち、認証部１４４から解除信号が送信された後は、シリンダキー２１２がキーシリンダ２１１に差し込まれると、エンジン２３への給電が行われる。

【００９９】また、第２の実施形態に係る認証システムは、車両履歴情報を用いた認証によって、車両を使用することが可能である。まず、入力部４１は、ユーザにより車両を使用する命令が入力されることにより、使用開始信号を出力する。使用開始信号は、カーナビゲーションシステム３に送信され、認証部１４４に入力される。これにより、情報処理部１４の認証部１４４は、認証処理を開始する。認証が成功した場合、認証部１４４は、

電力制御部２４に対して給電許可信号を送信する。給電許可信号に対して、電力制御部２４は、電源２２からエンジン２３への給電を開始する。なお、電力制御部２４は、認証部１４４からの給電禁止信号に対して認証部１４４からの給電許可信号を優先させる。これにより、給電禁止状態であったとしても、認証システムの認証によって車両を使用することが可能である。

【０１００】なお、第２の実施形態において、普段の乗車の際は、キーを用いた認証が行われる。すなわち、シリンダキー２１２がキーシリンダ２１１に差し込まれることにより、電力制御部２４は、電源２２からエンジン２３への給電を開始する。この場合、情報処理部１４の認証部１４４による認証処理は行われない。また、キーを用いた認証は、上記のようにキーの形状により認証を行うものの他、典型的にはイモビライザーのように、キーに特定の電子情報を含ませておくことにより認証を行うものであってもよい。

【０１０１】また、第２の実施形態においては、認証処理の際の質問および回答を行うために、入力端末４が用いられる。これは、車両のドアを開けるためにシリンダキー２１２が必要となる場合を考慮したものである。なお、他の実施形態においては、カーナビゲーションシステム３の入力部１１および出力部１２が用いられる形態であってもよい。また、カーナビゲーションシステム３の通信部１６と、入力端末４の通信部４３との間の通信は、例えば、Ｂｌｕｅｔｏｏｔｈにより実現することができるが、これに限るものではない。

【０１０２】次に、本発明に係る第３の実施形態について説明する。第３の実施形態に係る認証システムは、認証システムにおいて用いられる複数の認証方法の内の一つとして、車両履歴情報による認証が用いられる形態である。図１１は、第３の実施形態に係る認証システムの構成を示すブロック図である。図１１において、認証システムは、カーナビゲーションシステム５と、キーシリンダ２１１およびシリンダキー２１２と、電源２２と、エンジン２３と、電力制御部２４と、認証処理制御装置２５と、通報装置２６とを備えている。認証処理制御装置２５は、それぞれの認証方法について、正当なユーザであると認証された場合に行う処理を制御する。認証処理制御装置２５の動作の詳細は、図１２に示されている。通報装置２６は、ユーザに対して車両が使用されている旨を通報する。なお、図１１に示す認証システムは、第１の実施形態において用いられる構成要素と同様の構成要素を用いて実現することができる。従って、図１１において、図１と同じ構成要素には同一の参照符号を付し、説明を省略する。

【０１０３】次に、第３の実施形態に係る認証システムの動作を説明する。図１２は、図１１に示す認証システムにおいて用いられる認証方法と、認証結果に対する処理との関係を表す図である。第３の実施形態に係る認証システムにおいては、シリンダキー２１２を用いた認証方法および車両履歴情報を用いた認証方法が用いられる。図１２のように、シリンダキー２１２による認証が失敗した場合、認証処理制御装置２５は、車両を使用不可とする。さらに、この場合、認証処理制御装置２５は、通報処理を行う。また、シリンダキー２１２を用いた認証が成功し、車両履歴情報を用いた認証が失敗した場合、認証処理制御装置２５は、車両を使用可能とし、通報処理を行う。例えば、シリンダキー２１２が盗難されて、車両が不正に使用される場合でも、通報処理がなされる。また、シリンダキー２１２を用いた認証が成功し、車両履歴情報を用いた認証が成功した場合、認証処理制御装置２５は、車両を使用可能とし、通報処理を行わない。以下、認証処理制御装置２５の処理の詳細を説明する。

【０１０４】図１３は、図１１に示す認証処理制御装置２５における処理の流れを示すフローチャートである。認証処理制御装置２５における処理は、シリンダキー２１２がキーシリンダ２１１に差し込まれることにより開始される。まず、認証処理制御装置２５は、キーによる認証を行う（ステップＳ３１）。ここで、キーによる認証は、典型的にはイモビライザーのように、シリンダキー２１２に特定の電子情報を含ませておくことにより認証を行う。なお、キーによる認証の方法は、上記に限らず、例えば、機械的なシリンダキー２１２の形状がキーシリンダ２１１に合致するか否かにより認証を行うものであってもよい。

【０１０５】次に、認証処理制御装置２５は、ステップＳ３１における認証が成功したか否かを判定する（ステップＳ３２）。ステップＳ３１における認証が失敗した場合、認証処理制御装置２５は、車両の使用を禁止する（ステップＳ３３）。具体的には、認証処理制御装置２５は、電力制御部２４に対して給電許可信号を送信しない。従って、エンジン２３は、電源２２から給電が行われないため、始動しない。さらに、認証処理制御装置２５は、通報処理を行い（ステップＳ３４）、処理を終了する。ステップＳ３４の通報処理は、認証処理制御装置２５が通報装置２６に対して通報信号を送信することにより行われる。通報信号により、通報装置２６は、ユーザに対して車両が不正に使用されているおそれがある旨を通報する。具体的には、通報装置２６は、図示しないユーザの有する通信端末に対して車両が使用されている旨を通報する。なお、通報装置２６による通報の方法は上記に限るものではなく、ユーザに対して通知するものであれば、どのような構成であってもよい。

【０１０６】一方、ステップＳ３２の判定処理において、ステップＳ３１における認証が成功した場合、認証処理制御装置２５は、車両の使用を許可する（ステップＳ３５）。ステップＳ３５の処理は、認証処理制御装置２５が、電力制御部２４に給電許可信号を送信すること

により行われる。給電許可信号に応答して、電力制御部２４は、電源２２からエンジン２３への給電を開始する。

【０１０７】車両の使用を許可した後、認証処理制御装置２５は、カーナビゲーションシステム５に対して、車両履歴情報を用いた認証処理の開始を要求する（ステップＳ３６）。具体的には、認証処理制御装置２５は、カーナビゲーションシステム５の情報処理部１４に対して、認証開始信号を送信する。認証開始信号により、情報処理部１４の認証部１４４は、認証処理を開始する。ここで、認証部１４４による認証処理は、図７～図９に示す認証処理と同様である。また、図８に示すステップＳ２２０８および図９に示すステップＳ２３０３における認証が成功した場合の処理として、認証部１４４は、認証処理制御装置２５に対して認証が成功した旨の通知を行う。一方、図８に示すステップＳ２２１３および図９に示すステップＳ２３０６における、認証が失敗した場合の処理として、認証部１４４は、認証処理制御装置２５に対して認証が失敗した旨の通知を行う。

【０１０８】ステップＳ３６の後、認証処理制御装置２５は、車両履歴情報による認証が成功したか否かを判定する（ステップＳ３７）。ステップＳ３７における判定処理は、認証部１４４から認証が成功した旨の通知を受けたか否かにより行われる。ステップＳ３７における判定処理において、車両履歴情報による認証が失敗したと判定された場合、認証処理制御装置２５は、ステップＳ３４の処理を行い、処理を終了する。一方、車両履歴情報による認証が成功したと判定された場合、認証処理制御装置２５は、処理を終了する。

【０１０９】次に、本発明に係る第４の実施形態について説明する。第４の実施形態に係る認証システムは、車両履歴情報を用いた認証を、ユーザが有する端末を用いて行う形態である。図１４は、第４の実施形態に係る認証システムの構成を示すブロック図である。図１４において、認証システムは、車両に搭載されるカーナビゲーションシステム６と、キーシリンダ２１１およびシリンダキー２１２と、電源２２と、エンジン２３と、電力制御部２４と、認証端末７とを備えている。なお、図１４に示す認証システムは、第１の実施形態において用いられる構成要素と同様の構成要素を用いて実現することができる。従って、図１４において、図１と同じ構成要素には同一の参照符号を付し、説明を省略する。

【０１１０】カーナビゲーションシステム６は、入力部１１と、出力部１２と、記憶部１３と、情報処理部１４と、現在位置検出部１５と、通信部６６とを備えている。このように、カーナビゲーションシステム６は、第１の実施形態に係るカーナビゲーションシステム１の各構成要素に、通信部６６が加わった構成である。通信部６６は、認証端末７の通信部７５との間でデータの送受信を行う。

【０１１１】認証端末７は、入力部７１と、出力部７２と、記憶部７３、認証処理部７４と、通信部７５とを備えている。入力部７１は、ユーザが認証の際に質問に対する回答を入力するために用いられる。出力部７２は、認証を行う際の質問を、画像および音声により出力する。記憶部７３は、認証に必要となる車両履歴情報および個人情報を格納する。認証処理部７４は、車両履歴情報を用いた認証処理を行う。通信部７５は、カーナビゲーションシステム６の通信部６６との間で無線により通信を行う。

【０１１２】図１５は、図１４に示す認証端末７における、認証に必要な処理の流れを示すフローチャートである。まず、認証端末７は、認証に用いる車両履歴情報を、カーナビゲーションシステム６から取得する（ステップＳ４）。ステップＳ４の処理は、車両の使用が終了したとき、カーナビゲーションシステム６の記憶部１３に記憶されている車両履歴情報が、認証端末７に送信されることにより行われる。より具体的には、情報処理部１４は、車両のエンジンがＯＦＦになったとき、記憶部１３に記憶されている車両履歴情報を、通信部６６を介して認証端末７に送信する。以上により、認証端末７の記憶部７３には、車両履歴情報が記憶される。なお、ステップＳ４の処理を行うタイミングは、上記のタイミングに限らず、例えば、認証端末７により認証処理が行われる直前であってもよい。

【０１１３】車両履歴情報を取得した後、認証端末７は、認証処理を行う（ステップＳ５）。ステップＳ５の認証処理は、認証処理部７４において、ユーザにより入力部７１を用いて認証開始の命令が入力された場合に開始される。ここで、ステップＳ５の認証処理は、図７～図９に示す第１の実施形態に係る認証部１４４の認証処理と同様である。また、認証処理部７４は、図８に示すステップＳ２２０８および図９に示すステップＳ２３０３における認証が成功した場合の処理として、カーナビゲーションシステム６に対して、認証が成功した旨の通知を行う。なお、認証端末７からナビゲーションシステム６への認証が成功した旨の通知においては、典型的には、認証、電子署名、または暗号化が行われる。これにより、外部からの不正な操作が行われないようにする。

【０１１４】認証が成功した旨の通知を受けたカーナビゲーションシステム６の情報処理部１４は、電力制御部２４に対して給電禁止信号を送信する。給電禁止信号により、電力制御部２４は、シリンダキー２１２がキーシリンダ２１１に差し込まれることによる給電を禁止する。すなわち、認証部１４４からの給電禁止信号送信後は、シリンダキー２１２がキーシリンダ２１１に差し込まれても、エンジン２３への給電が行われない。なお、電力制御部２４は、認証部１４４からの給電禁止信号に対して認証部１４４からの給電許可信号を優先させる。これにより、給電禁止状態であったとしても、認証シス

テムの認証によって車両を使用することが可能である。

【０１１５】また、認証部１４４は、図８に示すステップＳ２２１３および図９に示すステップＳ２３０６における、認証が失敗した場合の処理として、警告を発する。具体的には、認証部１４４は、通信部６６を用いて認証端末７に対して認証が失敗した旨を通知する。通信部７５を介して通知を受けた認証処理部７４は、出力部４２に警告画像を表示させ、警告音を出力させる。

【０１１６】上述のように、第４の実施形態においては、車両の使用を禁止する場合に認証端末７が用いられる。ここで、他の実施形態においては、認証端末７は、車両を使用する場合に用いられる構成であってもよい。従って、第１の実施形態においても、第４の実施形態に係る認証システムにおいて用いられる認証端末７を用いることができる。この場合、ユーザは認証端末７により車外で認証を予め行っておき、車両乗車時に面倒な認証を行わないようにすることができる。

【０１１７】また、第４の実施形態においては、認証端末７における認証は、車両を使用するためまたは車両の使用を禁止するために行われる。ここで、他の実施形態においては、認証端末７の用途は、車両の使用に関するものに限らない。例えば、認証端末７が、料金の決済機能を有するものである場合、料金決済を行う際には、正当なユーザであることの認証が行われる。この場合、正当なユーザを認証するために、車両履歴情報を用いた認証を用いることができる。

【０１１８】また、第１の実施形態、第２の実施形態、第３の実施形態および第４の実施形態それぞれの電力制御部２４は、必ずしもエンジンへの電力供給を制限する装置である必要はない。電力制御部２４は、車両の使用を制御することができる方法、あるいは装置であればよい。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る認証装置を搭載した車両の構成を示すブロック図である。

【図２】図１に示す記憶部３の詳細な構成を示すブロック図である。

【図３】図２に示す車両履歴情報格納部１３２に格納される地点情報データテーブル１３２１の一例を示す図である。

【図４】図１に示す情報処理部４の詳細な構成を示すブロック図である。

【図５】第１の実施形態に係るカーナビゲーションシステム１における、認証に必要な処理の流れを示すフローチャートである。

【図６】図５のサブルーチンステップＳ１の詳細な処理を示すフローチャートである。

【図７】図５のサブルーチンステップＳ２の詳細な動作を示すフローチャートである。

【図８】図７のサブルーチンステップＳ２２の詳細な動作を示すフローチャートである。

【図９】図７のサブルーチンステップＳ２３の詳細な動作を示すフローチャートである。

【図１０】第２の実施形態に係る認証システムの構成を示すブロック図である。

【図１１】第３の実施形態に係る認証システムの構成を示すブロック図である。

【図１２】図１１に示す認証システムにおいて用いられる認証方法と、それぞれの認証結果に対する処理との関係を表す図である。

【図１３】図１１に示す認証処理制御装置２５における制御処理の流れを示すフローチャートである。

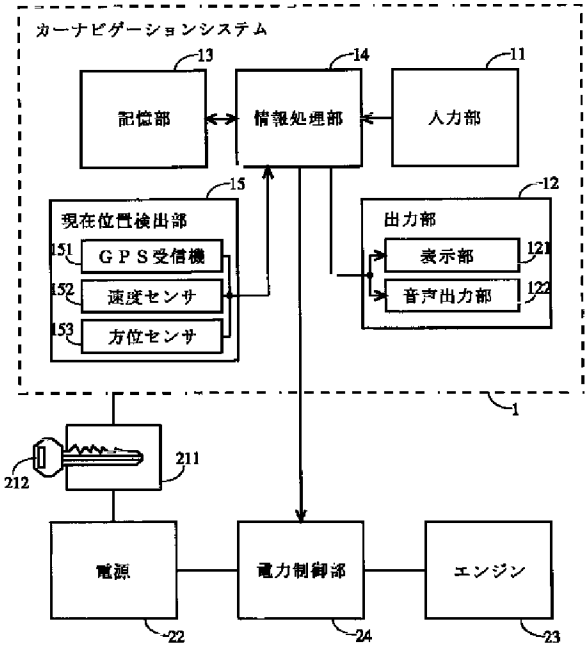
【図１４】第４の実施形態に係る認証システムの構成を示すブロック図である。

【図１５】図１４に示す認証端末７における、認証に必要な処理の流れを示すフローチャートである。

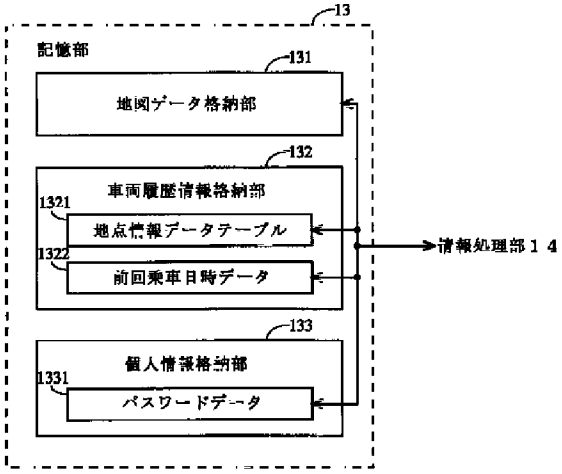
【符号の説明】

１，３，５，６…カーナビゲーションシステム
４…入力端末
７…認証端末
１１，４１，７１…入力部
１２，４２，７２…出力部
１３，７３…記憶部
１４…情報処理部
１５…現在位置検出部
１６，４３，６６，７５…通信部
２２…電源
２３…エンジン
２４…電力制御部
２５…認証処理制御装置
２６…通報装置
７４…認証処理部
１２１…表示部
１２２…音声出力部
１３１…地図データ格納部
１３２…車両履歴情報格納部
１３３…個人情報格納部
１４１…ロケーション部
１４２…経路探索部
１４３…経路案内部
１４４…認証部
１４５…車両履歴情報更新部
１５１…ＧＰＳ受信機
１５２…速度センサ
１５３…方位センサ
２１１…キーシリンダ
２１２…シリンダキー
１３２１…地点情報データテーブル
１３２２…前回乗車日時データ
１３３１…パスワードデータ

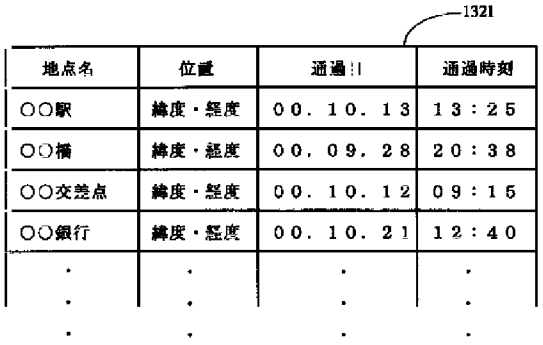
【図1】



【図2】

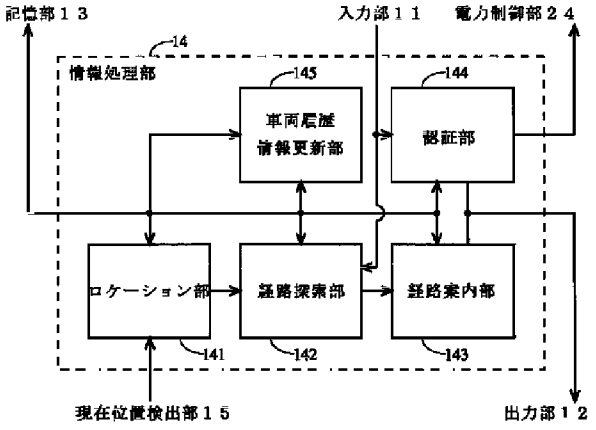


【図3】

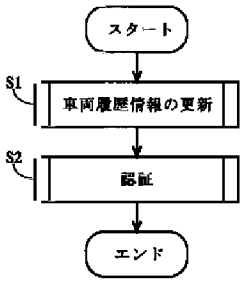


地点名	位置	通過日	通過時刻
○○駅	緯度・経度	00.10.13	13:25
○○橋	緯度・経度	00.09.28	20:38
○○交差点	緯度・経度	00.10.12	09:15
○○銀行	緯度・経度	00.10.21	12:40

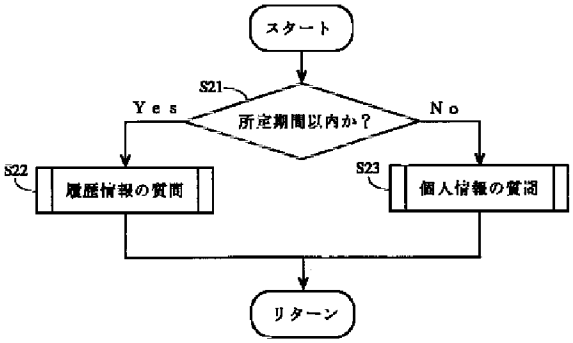
【図4】



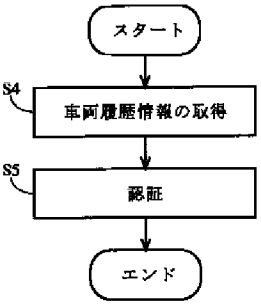
【図5】



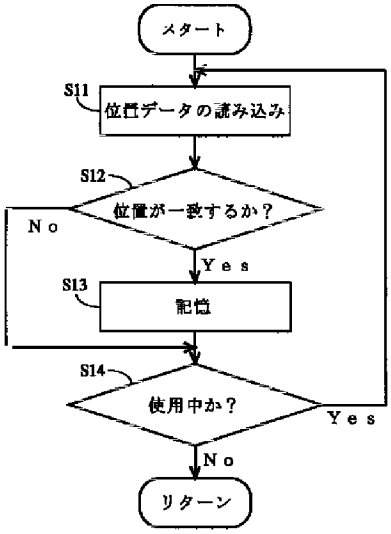
【図7】



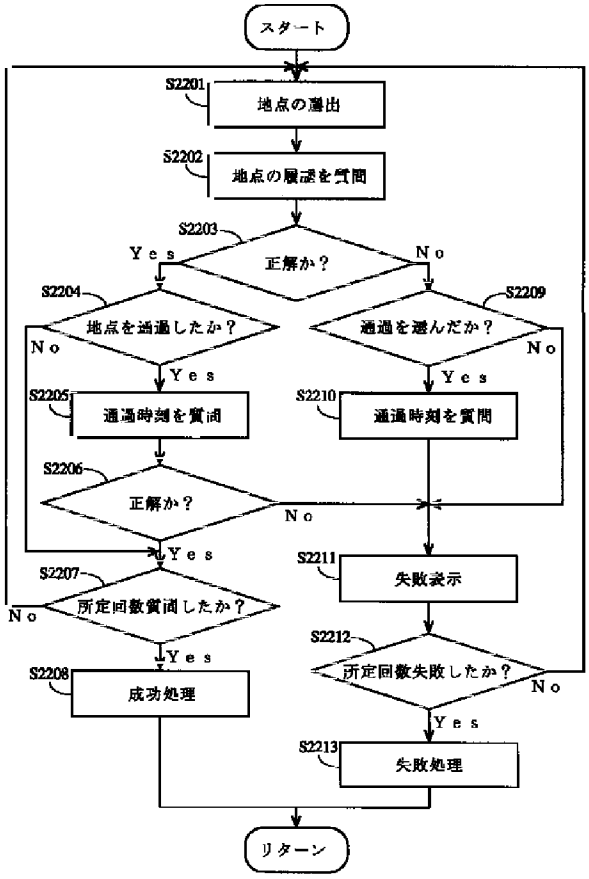
【図15】



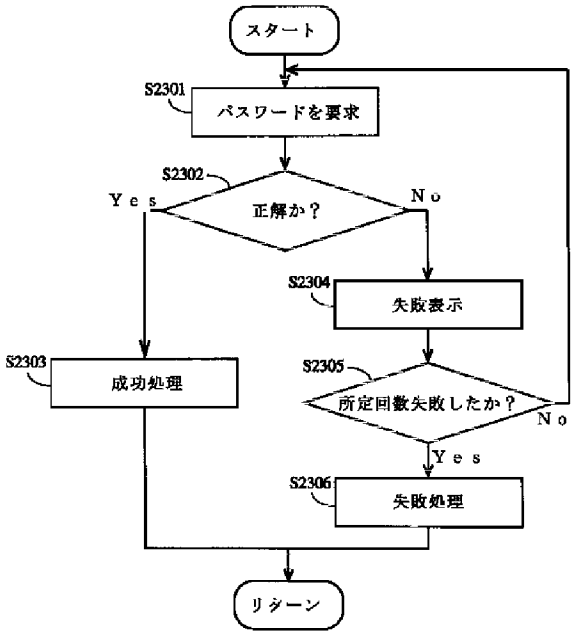
【図6】


スタート
S11
位置データの読み込み
S12
位置が一致するか？
No
Yes
S13
記憶
S14
使用中か？
Yes
No
リターン

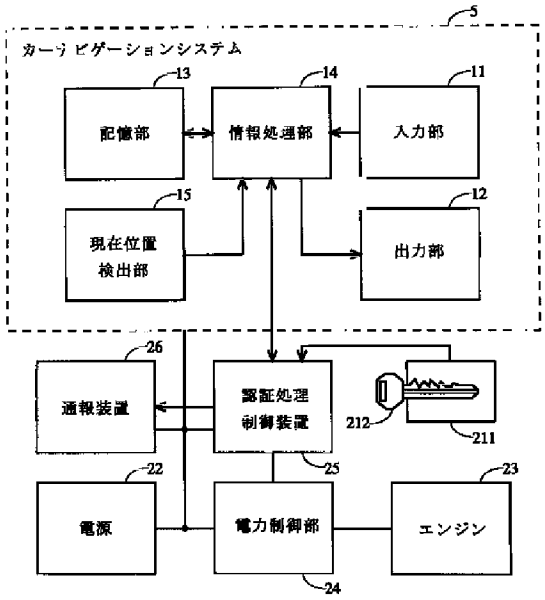
【図8】


スタート
S2201
地点の選出
S2202
地点の履歴を質問
S2203
正解か？
Yes
No
S2204
地点を通過したか？
No
Yes
S2205
通過時刻を質問
S2206
正解か？
No
Yes
S2207
所定回数質問したか？
No
Yes
S2208
成功処理
S2209
通過を避んだか？
No
Yes
S2210
通過時刻を質問
S2211
失敗表示
S2212
所定回数失敗したか？
No
Yes
S2213
失敗処理
リターン

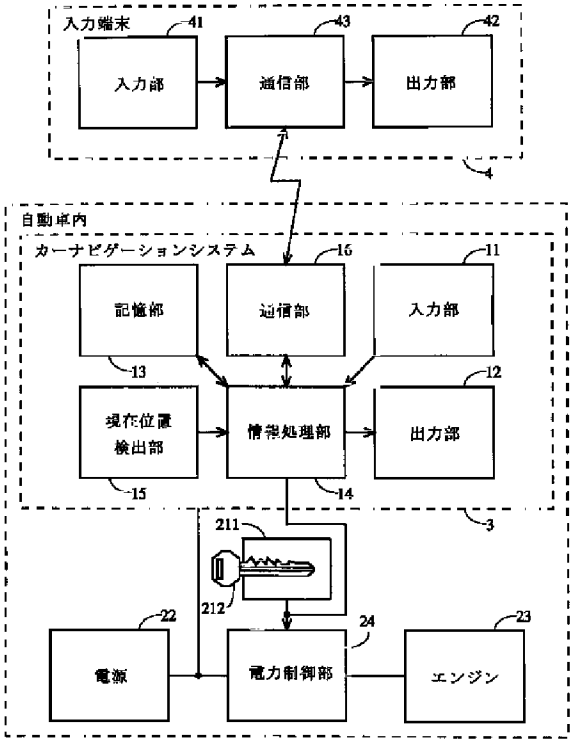
【図9】


スタート
S2301
パスワードを要求
S2302
正解か？
Yes
No
S2303
成功処理
S2304
失敗表示
S2305
所定回数失敗したか？
No
Yes
S2306
失敗処理
リターン

【図11】


5
カーナビゲーションシステム
13
記憶部
14
情報処理部
11
入力部
15
現在位置検出部
12
出力部
26
通報装置
認証処理制御装置
212
211
22
電源
25
電力制御部
23
エンジン
24

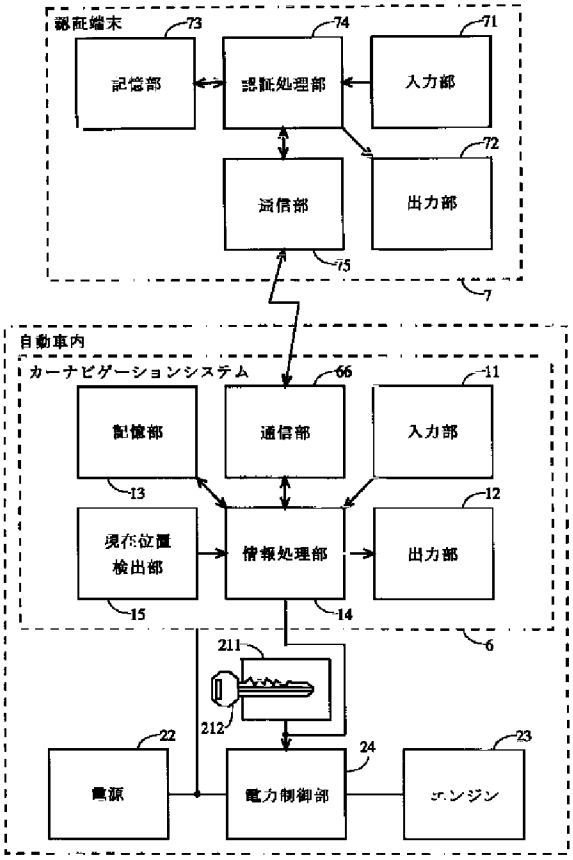
【図10】



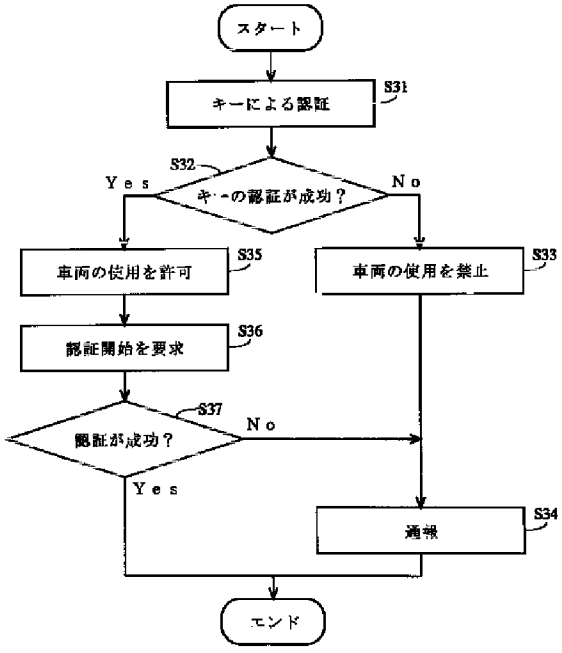
【図12】

		車両履歴情報による認証	
		成功	失敗
キーによる認証	成功	・車両使用可 ・通報不要	・車両使用可 ・通報要
	失敗	・車両使用不可 ・通報要	

【図14】



【図13】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ		(参考)
		Ｈ０４Ｌ 9/00	６７３Ａ	

(72)発明者 山下 敦士
大阪府門真市大字門真1006番地 松下電器産業株式会社内

(72)発明者 濱田 浩行
大阪府門真市大字門真1006番地 松下電器産業株式会社内

Ｆターム(参考) 2F029 AA02 AB07 AC02 AC08 AC14 AC16
5J104 AA07 KA01 KA07 KA09 NA05 PA16